CA ARCserve® Central Protection Manager

Guia do Usuário

r16

Referências a produtos da CA Technologies

Este documento faz referência aos seguintes produtos da CA Technologies:

- CA ARCserve® Backup
- CA ARCServe® D2D
- CA ARCserve® Replication and High Availability
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Protection Manager
- CA ARCserve® Central Reporting
- CA ARCserve® Central Virtual Standby

Entrar em contato com a CA

Para assistência técnica online e uma lista completa dos locais, principais horários de atendimento e números de telefone, entre em contato com o Suporte técnico pelo endereço http://www.ca.com/worldwide.

Links para suporte ao CA ARCserve Central Applications:

O CA Support online oferece um abrangente conjunto de recursos para solucionar seus problemas técnicos e fornece acesso fácil a importantes informações sobre o produto. Por meio do CA Support, você tem acesso fácil a consultas confiáveis que estão sempre disponíveis. Os links abaixo permitem acessar vários sites do CA Support disponíveis:

- **Entendendo o suporte --** O link abaixo fornece informações sobre programas de manutenção e ofertas de suporte, incluindo termos e condições, declarações, SLOs (Service-Level Objectives - Objetivos de Nível de Serviço) e horários de atendimento.

  https://support.ca.com/prodinfo/centappssupportofferings

- **Registrando-se para obter suporte --** O link abaixo o direciona para o formulário de registro online do CA Support que é usado para ativar o suporte ao produto.

  https://support.ca.com/prodinfo//supportregistration

- **Acessando o Suporte técnico --** O link abaixo o direciona à página de suporte ao CA ARCserve Central Applications.

  https://support.ca.com/prodinfo/arccentapps

Alterações na documentação

Esta documentação inclui comentários do usuário, aprimoramentos, correções e outras alterações secundárias para ajudar a melhorar a utilização e a compreensão do produto ou da própria documentação.

As seguintes atualizações na documentação foram feitas desde a última versão GA desta documentação:

Update 7

- Foram adicionadas opções de tarefa de mesclagem (na página 65). Esse tópico contém duas novas opções: Pausar tarefa de mesclagem (na página 65) e Retomar tarefa de mesclagem (na página 66) na tela Nó. Esses tópicos descrevem como pausar ou retomar uma tarefa de mesclagem para um determinado nó.
- A opção Especificar configurações de proteção (na página 82) foi atualizada. Esse tópico contém informações sobre as opções de configuração de retenção. Com as diretivas de retenção, especifique o número de pontos de recuperação ou de conjuntos de recuperação a serem retidos.
- A opção Especificar alertas por email (na página 121) foi atualizada. Esse tópico contém atualizações para os alertas de backup para tarefas de mesclagem. É possível receber um alerta para tarefas de mesclagem interrompidas, ignoradas, com falha ou paralisadas. Além disso, uma nova opção foi adicionada para alertá-lo sobre tarefas de mesclagem bem-sucedidas.

Update 6

- Configurar programações de detecção (na página 34) atualizada. Este tópico inclui agora uma lista do Active Directory para que você possa visualizar ao configurar uma programação para detectar nós.
- Definir configuração de email e alerta (na página 34) atualizado O título foi renomeado e o tópico foi atualizado para incluir os alertas sobre os nós detectados.
- Atualizar nós (na página 61) atualizados. O tópico descreve como é possível atualizar vários nós simultaneamente usando as credenciais existentes ou especificando novas credenciais. Também é possível forçar o servidor para gerenciar os nós selecionados.
- Adicionar grupos de nós (na página 71) atualizados. Este tópico substitui o grupo de nó "Não atribuído" com "Nós sem uma diretiva" e substitui o grupo de nó "Sem grupo" com "Nós sem um grupo".
- Implantar o CA ARCserve D2D para nós (na página 77) atualizado. Esse tópico foi atualizado para incluir a última versão do CA ARCserve D2D ao implantar em um nó e suporte versões menores do CA ARCserve D2D. Também inclui um novo botão chamado Marcar/Desmarcar tudo para selecionar nós.

- Especificar destinos de cópia de arquivo (na página 107) atualizado. Esse tópico foi atualizado para incluir a Fujitsu Cloud (Windows Azure) como outro tipo de fornecedor para a configuração da nuvem.
- Nesta versão atualizada, é possível exibir o status da implantação de diretivas na coluna Diretiva.

Update 5

- Compreendendo a tela Gerenciamento de nós (na página 53). A captura de tela Exibição de nós foi removida deste tópico, devido a alterações contínuas na interface de usuário.
- Adicionar grupos de nós (na página 71). Esse tópico foi atualizado para incluir os filtros Nome do grupo e Nome do nó.
- Implantar o CA ARCserve D2D em nós (na página 77). Esse tópico foi atualizado para incluir um filtro Nome de nó e Grupo na tela Implantação do D2D.
- Atribuir e remover a atribuição de nós de diretivas (na página 133). Esse tópico foi atualizado para incluir os filtros Nome do nó e Grupo na tela Atribuir/Remover a atribuição de diretivas.

Update 4

- Como desinstalar o Gerenciador do CA ARCserve Central Protection (na página 21) adicionado. Este cenário descreve os métodos que você pode usar para desinstalar o aplicativo.
- Usando o Gerenciador do CA ARCserve Central Protection para fazer backup dos nós do CA ARCserve D2D (na página 46) adicionado. Este cenário descreve como criar uma diretiva de backup básica que permite fazer backup dos nós do CA ARCserve D2D.
- Executar um backup agora (na página 135) adicionado. Este tópico descreve como executar uma tarefa de backup ad hoc.
- Exibir informações de status da tarefa (na página 137) adicionado. Este tópico descreve como exibir informações em tempo real sobre as tarefas de backup em andamento.
- Atualização de todos os tópicos que descrevem como restaurar dados (na página 137). Agora, você envia tarefas de restauração diretamente na tela Nó.
- Alterar o protocolo de comunicação do servidor (na página 159) adicionado. Este tópico descreve como alterar o protocolo de comunicação usado pelos componentes do CA ARCserve Central Applications de HTTP para HTTPS e de HTTPS para HTTP usando um arquivo em lote.

Update 1

- Integrando o Gerenciador do CA ARCserve Central Protection às ferramentas do servidor de gerenciamento de TI (na página 161) adicionado. Esta seção descreve como integrar o Gerenciador do CA ARCserve Central Protection às ferramentas de gerenciamento da infraestrutura do servidor de gerenciamento de TI. Por exemplo, Nimsoft e Kaseya.

Índice

Capítulo 4: Usando o Gerenciador do CA ARCserve Central Protection 45

Capítulo 5: Integração do Gerenciador do CA ARCserve Central Protection às ferramentas do servidor de gerenciamento de TI 161

Capítulo 6: Solução de problemas do Gerenciador do CA ARCserve Central Protection 177

Índice remissivo 203

Capítulo 1: Introdução ao Gerenciador do CA ARCserve Central Protection

Esta seção contém os seguintes tópicos:

Introdução

O CA ARCserve Central Applications combina as principais tecnologias de gerenciamento e proteção de dados com um ecossistema de aplicativos de destino que funcionam em uníssono para possibilitar proteção, cópia, movimentação e transformação de dados, no local e remotamente, em ambientes globais.

O CA ARCserve Central Applications é fácil de usar, gerenciar e instalar. Ele fornece às empresas controle automatizado de suas informações para tomarem decisões conscientes sobre o acesso, a disponibilidade e a segurança de seus dados, com base no valor comercial geral.

Entre os aplicativos oferecidos pelo CA ARCserve Central Applications, está o Gerenciador do CA ARCserve Central Protection. O Gerenciador do CA ARCserve Central Protection permite gerenciar ambientes do CA ARCserve D2D e do CA ARCserve Backup de um local central. Aplicativos individuais fornecem um grau de gerenciamento de nó limitado, enquanto o Gerenciador do CA ARCserve Central Protection permite fazer o seguinte:

- Adicionar um ou vários nós
- Detectar nós por meio do servidor do active Directory
- Detectar e adicionar máquinas virtuais gerenciadas por um hipervisor
- Detectar o aplicativo em servidores adicionados
- Criar e atribuir diretivas do CA ARCserve D2D
- Enviar uma tarefa de restauração para o CA ARCserve D2D gerenciado
- Sincronizar dados de servidores gerenciados do CA ARCserve Backup e do CA ARCserve D2D
- Implantar o CA ARCserve D2D

Funcionamento do aplicativo

O Gerenciador do CA ARCserve Central Protection permite exibir e gerenciar nós protegido de um local central.

Inicie o Gerenciador do CA ARCserve Central Protection selecionando o menu Iniciar > Todos os Programas > CA > ARCserve Central Applications > Gerenciador do CA ARCserve Central Protection. A página inicial do Gerenciador do CA ARCserve Central Protection é exibida, onde você pode acessar qualquer função do Gerenciador do CA ARCserve Central Protection usando os seguintes recursos de navegação:

- **Nó -** permite usar várias ferramentas para gerenciar nós e grupos de nós, detectar nós, implantar o CA ARCserve D2D para nós e sincronizar dados.
- **Diretivas -** permite adicionar, editar, excluir e atribuir diretivas do CA ARCserve D2D. Este recurso exibe os detalhes da diretiva e permite atribuir ou remover a atribuição de um nó de sua diretiva do CA ARCserve D2D correspondente.
- **Configuração -** permite definir as configurações do banco de dados, sincronização de dados do CA ARCserve Backup, SRM, detecção, configuração de email, configuração da atualização, preferências, conta de administrador, implantação do D2D e servidor de gerenciamento de TI.
- **Exibir logs** - permite exibir logs de atividades para cada nó individual. O Gerenciador do CA ARCserve Central Protection exibe todas as mensagens de log associadas a esse nó. É possível filtrar a lista especificando a gravidade das mensagens exibidas (Todas, Informações, Erros, Avisos ou Erros e avisos), o tipo de módulo (Todos, Comum, Importar nós a partir da detecção, Importar nós do HyperVisor, Importar nós do arquivo, Gerenciamento de diretivas, Sincronização do CA ARCserve Backup, Sincronização do CA ARCserve D2D, Atualizações do CA ARCserve D2D, Atualizações e Enviar tarefas de backup do CA ARCserve D2D) ou o nome do nó.

Biblioteca do CA ARCserve Central Applications

Os mesmos tópicos contidos no sistema de ajuda do CA ARCserve Central Applications também estão disponíveis como um Guia do Usuário em PDF. A versão mais recente deste guia e o sistema de ajuda podem ser acessados a partir da Biblioteca do CA ARCserve Central Applications.

Os arquivos de Notas da Versão do CA ARCserve Central Applications contém informações relacionadas aos requisitos do sistema, suporte ao sistema operacional, suporte à recuperação de aplicativos e outras informações que podem ser necessárias antes de instalar este produto. Além disso, estes arquivos contêm uma lista de problemas conhecidos os quais você deve saber antes de usar o CA ARCserve Central Applications. A versão mais recente de Notas da Versão pode ser acessada a partir da Biblioteca do CA ARCserve Central Applications.

Capítulo 2: Instalando o Gerenciador do CA ARCserve Central Protection

Esta seção contém os seguintes tópicos:

Tarefas essenciais da instalação

Antes de instalar o aplicativo, complete as seguintes tarefas essenciais:

- Examine as Notas da versão. As Notas da Versão contêm uma descrição de requisitos do sistema, sistemas operacionais suportados e uma lista de problemas conhecidos nesta release do Gerenciador do CA ARCserve Central Protection.
- Verifique se o sistema atende aos requisitos de software e hardware que são necessários para instalar o aplicativo.
- Verifique se sua conta do Windows tem privilégios de administrador ou equivalente para instalar o software nos computadores em que planeja instalar o Gerenciador do CA ARCserve Central Protection.
- Verifique se você tem em mãos os nomes de usuário e senhas dos computadores em que você está instalando o aplicativo.

- Verifique se o servidor onde deseja instalar o Gerenciador do CA ARCserve Central Protection e os nós onde deseja implantar diretivas podem se comunicar uns com os outros usando seus nomes de host. Para verificar se os servidores e nós do Gerenciador do CA ARCserve Central Protection podem se comunicar uns com os outros, proceda da seguinte forma:
  - No servidor do Gerenciador do CA ARCserve Central Protection,execute o comando ping nos nós usando seus respectivos nomes de host.
  - Nos nós que deseja proteger, execute o comando ping no servidor do Gerenciador do CA ARCserve Central Protection usando seu nome de host.
- O Gerenciador do CA ARCserve Central Protection permite instalar o CA ARCserve D2D r16 e atualizar o CA ARCserve D2D r15 para o CA ARCserve D2D r16 em nós remotos usando o utilitário Implantar. Para fazer backup de dados em nós remotos usando o CA ARCserve D2D r16, é preciso obter as licenças do CA ARCserve D2D r16 e aplicá-las nos nós. Se não aplicar as licenças em 31 dias da data que você instalou ou atualizou para o CA ARCserve D2D r16 nos nós, o CA ARCserve D2D irá parar de funcionar.
- A mídia de instalação do Gerenciador do CA ARCserve Central Protection contém o Microsoft SQL Server 2008 R2 Express Edition, que é o aplicativo de banco de dados mínimo necessário para oferecer suporte ao banco de dados do Gerenciador do CA ARCserve Central Protection. Se desejar usar o Microsoft SQL Server para oferecer suporte ao banco de dados do Gerenciador do CA ARCserve Central Protection, instale o Microsoft SQL Server no servidor do Gerenciador do CA ARCserve Central Protection ou em servidor remoto antes de instalar o Gerenciador do CA ARCserve Central Protection. Se a rotina de instalação detectar uma versão do Microsoft SQL Server que não seja suportada, a instalação de rotina falhará. Para obter mais informações sobre as versões suportadas do Microsoft SQL Server, consulte as Notas da versão.

Considerações sobre a instalação

Antes de instalar o Gerenciador do CA ARCserve Central Protection, observe as seguintes considerações de instalação:

- O pacote de instalação do CA ARCserve Central Applications instala um módulo chamado Servidor do CA ARCserve Central Applications. O servidor do CA ARCserve Central Applications é um módulo que é comum a todos os aplicativos CA ARCserve Central Applications. O módulo contém o serviço web, os binários e configurações que permitem que o CA ARCserve Central Applications se comunique com os outros.

  Ao instalar o CA ARCserve Central Applications, o pacote de instalação instala o módulo do servidor do CA ARCserve Central Applications antes de instalar os componentes do produto. Se for necessário aplicar um patch ao CA ARCserve Central Applications, ele atualizará o módulo antes de atualizar os componentes do produto.

- Ao implantar o CA ARCserve D2D em nós remotos, o Gerenciador do CA ARCserve Central Protection instala o VDDK (VMware Virtual Disk Development Kit) 1.2.1 nos nós de destino. A mídia de instalação do Gerenciador do CA ARCserve Central Protection inclui os arquivos de instalação que são necessários para instalar o VDDK (VMware Virtual Disk Development Kit) 1.2.1 no servidor do Gerenciador do CA ARCserve Central Protection e no nó de destino. Portanto, você não precisa fazer download dos arquivos de instalação do VDDK do site da VMware para implantar o CA ARCserve D2D em nós remotos.

Instalar o Gerenciador do CA ARCserve Central Protection

O Assistente de instalação ajuda a orientá-lo durante todo o processo de instalação de um ou mais CA ARCserve Central Applications.

Observação: antes de instalar o aplicativo, consulte o arquivo Notas da versão e verifique se todas as tarefas descritas em Tarefas de pré-requisito foram concluídas.

Para instalar o Gerenciador do CA ARCserve Central Protection

1. Baixe o pacote de instalação do CA ARCserve Central Applications para o computador no qual você deseja instalar o aplicativo e clique duas vezes no Arquivo de instalação.

   O pacote de instalação extrai seu conteúdo para o computador e, em seguida, a caixa de diálogo Componentes essenciais é aberta.

2. Clique em Instalar na caixa de diálogo Componentes essenciais.

   Observação: a caixa de diálogo Componentes essenciais será exibida somente se o programa de instalação não detectar os componentes essenciais instalados no computador.

   Depois que o programa de instalação instalar os componentes essenciais, a caixa de diálogo do Contrato de licença é aberta.

3. Preencha os campos necessários da caixa de diálogo Contrato de licença e clique em Avançar.

   A caixa de diálogo Configuração é aberta.

4. Na caixa de diálogo de Configuração, preencha o seguinte:

   - **Componentes -** especifique os aplicativos que você deseja instalar.

     Observação: se instalar esse aplicativo usando o conjunto do pacote de instalação, você poderá instalar vários aplicativos.

   - **Local -** aceite o local padrão da instalação ou clique em Procurar para especificar um local de instalação alternativo. O diretório padrão é o seguinte:

     `C:\Arquivos de programas\CA\ARCserve Central Applications\BIN`

   - **Informações do disco -** verifique se o disco rígido tem espaço livre suficiente para instalar os aplicativos.

   - **Nome do administrador do Windows -** especifique o nome de usuário da conta de administrador do Windows usando a seguinte sintaxe:

     `Domínio\Nome do usuário`

   - **Senha -** especifique a senha da conta do usuário.

   - **Especificar o número da porta -** especifique o número de porta que deseja usar para se comunicar com a interface do usuário baseada na web. Como prática recomendada, você deve aceitar o número de porta padrão. O número da porta padrão é o seguinte:

     `8015`

     Observação: se desejar especificar um outro número de porta, os números de porta disponíveis vão de 1024 a 65535. Para que você especifique um outro número de porta, verifique se o número de porta especificado está livre e disponível para uso. A instalação impede que você instale o aplicativo usando uma porta que não esteja disponível para uso.

   - **Usar HTTPS para a comunicação web** - especifique usar a comunicação HTTPS para a transmissão de dados. Essa opção não vem selecionada por padrão.

     Observação: a comunicação HTTPS (segura) fornece um nível maior de segurança do que a comunicação HTTP. O HTTPS é o protocolo de comunicação recomendado se você transmite informações confidenciais na rede.

- **Permitir que o programa de instalação registre como exceções os serviços/programas do CA ARCserve Central Applications no Firewall do Windows -** verifique se a caixa de seleção para essa opção está marcada. As exceções do firewall são necessárias para configurar e gerenciar o CA ARCserve Central Applications por meio de computadores remotos.

  Observação: para usuários locais, não é preciso registrar as exceções do firewall.

Clique em Avançar.

A caixa de diálogo Configurações de banco de dados é aberta.

5. Na caixa de diálogo Configurações do banco de dados, clique na lista suspensa ao lado de Escolha o tipo de BD e especifique um dos itens abaixo.

   - Banco de dados padrão do ARCserve Central Applications
   - Microsoft SQL Server

   Depois que você especificar um tipo de banco de dados, as opções necessárias para o banco de dados especificado são exibidas na caixa de diálogo Configurações do banco de dados.

6. Siga um destes procedimentos:

   - **Banco de dados padrão do ARCserve Central Applications -** preencha os seguintes campos na caixa de diálogo Configurações do banco de dados:

     - **Especifique o caminho de instalação -** especifique o local onde você deseja instalar o banco de dados padrão do CA ARCserve Central Applications. É possível aceitar o caminho padrão ou especificar um caminho alternativo.
     - **Especifique o caminho do arquivo de dados -** especifique o local onde deseja instalar o arquivo de dados para o banco de dados padrão do CA ARCserve Central Applications. É possível aceitar o caminho padrão ou especificar um caminho alternativo.

     Observação: o banco de dados padrão do CA ARCserve Central Applications não tem suporte para comunicação remota. Portanto, instale o banco de dados padrão e o arquivo de dados no computador em que você está instalando o aplicativo.

- **Bancos de dados padrão do SQL Server -** preencha os seguintes campos na caixa de diálogo Configurações do banco de dados:
  - **Tipo de SQL Server -** especifique o tipo de comunicação que o aplicativo deve usar para se comunicar com o banco de dados do SQL Server.

    Local: especifique Local quando o aplicativo e SQL Server estão instalados no mesmo computador.

    Remoto: especifique Remoto quando o aplicativo e o SQL Server estão instalados em computadores diferentes.
  - **Nome do SQL Server--**Se o Tipo de SQL Server especificado for remoto, especifique o nome do SQL Server. Se o SQL Server for usado localmente, selecione o servidor na lista suspensa.
  - **Segurança -** especifique o tipo de credenciais que você deseja usar para autenticação com o SQL Server.

    Usar segurança do Windows - especifique Usar segurança do Windows para autenticar usando suas credenciais do Windows.

    Usar segurança do SQL Server - especifique Usar segurança do SQL Server para autenticar usando credenciais do SQL Server. Em seguida, especifique a ID de logon e a senha para a conta do SQL Server.
  - **Substituir banco de dados existente--** especifique a opção Substituir banco de dados se deseja permitir que o programa de instalação detecte e substitua banco de dados do CA ARCserve Central Applications.

   Clique em Instalar.

   Depois que o processo de instalação for concluído, a caixa de diálogo Relatório de instalação será aberta.

7. A caixa de diálogo Relatório de instalação resume a instalação. Se deseja verificar se há atualizações para o aplicativo agora, clique em Verificar se há atualizações e clique em Concluir.

O aplicativo está instalado.

Instalar o Gerenciador do CA ARCserve Central Protection de modo silencioso

O CA ARCserve Central Applications permite instalar o Gerenciador do CA ARCserve Central Protection de modo silencioso. O processo de instalação silenciosa elimina a necessidade de interação com o usuário. As etapas a seguir descrevem como instalar o aplicativo no modo silencioso usando a linha de comando do Windows.

Para instalar o Gerenciador do CA ARCserve Central Protection de modo silencioso

1. Abra a linha de comando do Windows no computador onde deseja iniciar o processo de instalação silenciosa.
2. Faça download do pacote de instalação de auto-extração do CA ARCserve Central Applications para o computador.

   Inicie o processo de instalação silenciosa usando a seguinte sintaxe da linha de comando:

   ```
   "CA ARCserve Central Applications Setup.exe" /s /v"/q -Path:<INSTALLDIR>
   -Port:<PORT> -U:<UserName> -P:<Password> -Products:<ProductList>"
   ```

   Utilização:

   s

   Permite executar o pacote de arquivo executável no modo silencioso.

   v

   Permite especificar outras opções de linha de comando.

   q

   Permite instalar o aplicativo no modo silencioso.

   -Path:<INSTALLDIR>

   (Opcional) Permite especificar o caminho de instalação de destino.

   Exemplo:

   ```
   -Path:\"C:\Arquivos de Programas\CA\ARCserve Central Applications\"
   ```

   Observação: se o valor de INSTALLDIR tiver um espaço, coloque o caminho entre barras invertidas e aspas. Além disso, o caminho não pode terminar com um caractere de barra invertida.

   -Port:<PORT>

   (Opcional) Permite especificar o número da porta para comunicação.

   Exemplo:

   ```
   -Porta:8015
   ```

-U:<UserName>

Permite especificar o nome de usuário a ser usado para instalar e executar o aplicativo.

Observação: o nome de usuário deve ser uma conta administrativa ou uma conta com privilégios administrativos.

-P:<Password>

Permite especificar a senha para o nome de usuário.

-Products:<ProductList>

(Opcional) Permite especificar uma instalação do CA ARCserve Central Applications de modo silencioso. Se você não especificar um valor para o argumento, o processo de instalação silenciosa instalará todos os componentes do CA ARCserve Central Applications.

CA ARCserve Central Host-Based VM Backup

VSPHEREX64

Gerenciador do CA ARCserve Central Protection

CMX64

CA ARCserve Central Reporting

REPORTINGX64

CA ARCserve Central Virtual Standby

VCMX64

Todos os aplicativos CA ARCserve Central Applications

TODOS

Observação: os exemplos a seguir descrevem a sintaxe necessária para instalar um, dois, três ou todos os aplicativos CA ARCserve Central Applications silenciosamente:

```
-Products:<CMX64>
-Products:CMX64,VCMX64
-Products:CMX64,VCMX64,REPORTINGX64
-Products:<ALL>
```

O aplicativo foi instalado de modo silencioso.

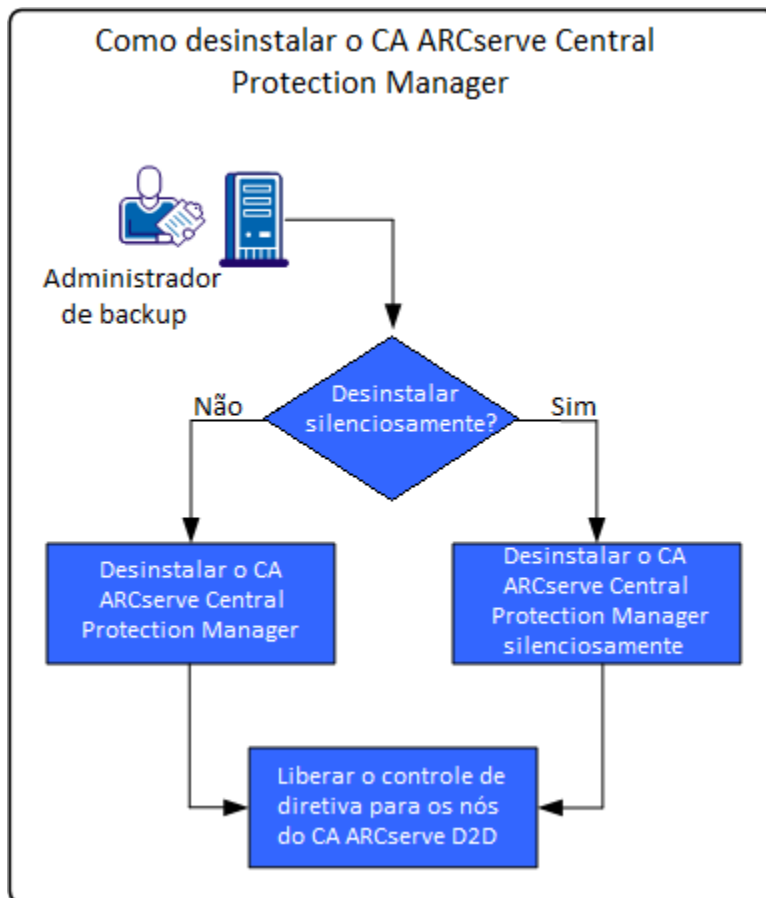
Como desinstalar o Gerenciador do CA ARCserve Central Protection

Você pode instalar o Gerenciador do CA ARCserve Central Protection usando os seguintes métodos:

- Desinstalação padrão - este método usa o Painel de Controle do Windows para desinstalar o aplicativo.
- Desinstalação silenciosa - este método permite executar uma desinstalação autônoma usando a linha de comando do Windows.

Removendo a atribuição de diretivas

Como prática recomendada, remova a atribuição de todas as diretivas dos nós aos quais elas estão atribuídas antes de desinstalar o aplicativo. Recomendamos essa abordagem porque você não pode especificar as configurações de backup do CA ARCserve D2D no nó enquanto uma diretiva do Gerenciador do CA ARCserve Central Protection estiver atribuída ao nó. Além disso, você não pode remover a atribuição de diretivas de nós depois de desinstalar o aplicativo. O CA ARCserve D2D fornece um utilitário de linha de comando que permite remover a atribuição de diretivas de nós depois de desinstalar o aplicativo.

O diagrama a seguir ilustra como desinstalar o aplicativo:

Tarefa	Consultar o tópico
Executar uma desinstalação padrão usando o Painel de Controle do Windows.	Desinstalar o Gerenciador do CA ARCserve Central Protection (na página 23).
Executar uma desinstalação silenciosa usando a linha de comando do Windows.	Desinstalar o Gerenciador do CA ARCserve Central Protection de modo silencioso (na página 24).
Remover a atribuição de diretivas de nós após a desinstalação do Gerenciador do CA ARCserve Central Protection.	Liberar o controle de diretiva para os nós do CA ARCserve D2D (na página 25).

Desinstalar o Gerenciador do CA ARCserve Central Protection

É possível desinstalar o Gerenciador do CA ARCserve Central Protection usando Programas e Recursos, localizado no Painel de Controle do Windows.

Siga estas etapas:

1. Efetue logon no computador de onde deseja desinstalar o aplicativo.

   Observação: efetue logon usando uma conta administrativa ou uma conta com privilégios administrativos.

2. No menu Iniciar do Windows, clique em Iniciar e, em seguida, clique em Painel de Controle para abrir o Painel de Controle do Windows.

3. Clique em Programas e Recursos para abrir a janela Desinstalar ou alterar um programa.

4. Localize e clique em Gerenciador do CA ARCserve Central Protection.

   Clique com o botão direito do mouse no aplicativo e clique em Desinstalar no menu pop-up.

   Siga as instruções na tela para desinstalar o aplicativo.

O aplicativo será desinstalado.

Desinstalar o Gerenciador do CA ARCserve Central Protection de modo silencioso

O CA ARCserve Central Applications permite desinstalar o Gerenciador do CA ARCserve Central Protection de modo silencioso. O processo de instalação silenciosa elimina a necessidade de interação com o usuário. As etapas a seguir descrevem como desinstalar o aplicativo no modo silencioso usando a linha de comando do Windows.

Siga estas etapas:

1. Efetue logon no computador de onde deseja desinstalar o aplicativo.

   Observação: efetue logon usando uma conta administrativa ou uma conta com privilégios administrativos.

2. Abra a linha de comando do Windows e execute o seguinte comando para iniciar o processo de desinstalação silenciosa:

   ```
   <INSTALLDIR>%\Setup\uninstall.exe /q /p <ProductCode>
   ```

   Ou

   ```
   <INSTALLDIR>%\Setup\uninstall.exe /q /ALL
   ```

   Exemplo: a sintaxe a seguir permite desinstalar o aplicativo de modo silencioso.

   ```
   "%ProgramFiles%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p
   {CAED05FE-D895-4FD5-B964-001928BD2D62}
   ```

   Utilização:

   <INSTALLDIR>

   Permite especificar o diretório no qual o aplicativo está instalado.

   Observação: execute a sintaxe que corresponde à arquitetura do sistema operacional do computador.

   <ProductCode>

   Permite especificar o aplicativo a ser desinstalado silenciosamente. Use os seguintes códigos de produtos para desinstalar o CA ARCserve Central Applications de modo silencioso.

   Gerenciador do CA ARCserve Central Protection

   {CAED05FE-D895-4FD5-B964-001928BD2D62}

   CA ARCserve Central Host-Based VM Backup

   {CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}

   CA ARCserve Central Reporting

   {CAED8DA9-D9A8-4F63-8689-B34DEEEEC542}

   CA ARCserve Central Virtual Standby

   {CAED4835-964B-484B-A395-E2DF12E6F73D}

O aplicativo é desinstalado de modo silencioso.

Liberar o controle de diretiva para os nós do CA ARCserve D2D

O processo de desinstalação do Gerenciador do CA ARCserve Central Protection não remove a atribuição de diretivas de backup dos nós do CA ARCserve D2D. Esse comportamento impede que você especifique as configurações de backup diretamente nos nós do CA ARCserve D2D depois de desinstalar o Protection Manager. Como prática recomendada, você pode remover a atribuição de todas as diretivas dos nós aos quais elas estão atribuídas antes de desinstalar o aplicativo. Se não usar essa prática, você pode liberar o controle de diretiva para os nós usando um utilitário projetado especificamente para esse propósito.

Siga estas etapas:

1. Efetue logon no nó do CA ARCserve D2D.
2. Abra Linha de comando do Windows e vá para o seguinte diretório:

   ```
   C:\Arquivos de Programas\CA\ARCserve D2D\BIN
   ```

3. Execute ARCCentralAppMgrUtility.exe usando a seguinte sintaxe:

   ```
   ARCCentralAppMgrUtility.exe -clean pm|hbvb|vs [-debug]
   ```

   pm|hbvb|vs

   Defina o aplicativo que deseja liberar do controle do nó do CA ARCserve D2D. Especifique um dos seguintes argumentos:

   pm

   Gerenciador do CA ARCserve Central Protection

   hbvb

   CA ARCserve Central Host-Based VM Backup

   vs

   CA ARCserve Central Virtual Standby

   -debug

   A opção -debug não é necessária. Com essa opção especificada, o utilitário gera um arquivo de log de depuração que é armazenado no seguinte diretório:

   ```
   <D2D_Home>\Log\ARCCentralAppMgrUtility.log
   ```

   Exemplo: o exemplo a seguir descreve a sintaxe para liberar o controle de diretiva para o nó.

   ```
   ARCCentralAppMgrUtility.exe -clean pm
   ```

O controle de diretiva é liberado para o nó.

Como o processo de instalação afeta os sistemas operacionais

O processo de instalação do CA ARCserve Central Applications atualiza vários componentes do sistema operacional Windows, usando um mecanismo de instalação denominado MSI (Microsoft Installer Package). Os componentes incluídos no MSI permitem que o CA ARCserve Central Applications execute ações personalizadas para instalação, atualização e desinstalação do CA ARCserve Central Applications.

A tabela a seguir descreve as ações personalizadas e os componentes afetados:

Observação: todos os pacotes MSI do CA ARCserve Central Applications chamam os componentes relacionados nesta tabela quando você instala e desinstala o CA ARCserve Central Applications.

Componente	Descrição
CallAllowInstall	Permite ao processo de instalação verificar condições relativas à instalação atual do CA ARCserve Central Applications.
CallPreInstall	Permite ao processo de instalação ler e gravar propriedades do MSI. Por exemplo, ler o caminho de instalação do CA ARCserve Central Applications no MSI.
CallPostInstall	Permite ao processo de instalação executar várias tarefas relativas à instalação. Por exemplo, registrar o CA ARCserve Central Applications no Registro do Windows.
CallAllowUninstall	Permite ao processo de desinstalação verificar condições relativas à instalação atual do CA ARCserve Central Applications.
CallPreUninstall	Permite ao processo de desinstalação executar várias tarefas relativas à desinstalação. Por exemplo, cancelar o registro do CA ARCserve Central Applications no Registro do Windows.
CallPostUninstall	Permite que o processo de desinstalação execute várias tarefas depois de desinstalar os arquivos instalados. Por exemplo, a remoção dos arquivos restantes.
ShowMsiLog	Exibe o arquivo de log do Windows Installer no Bloco de notas, caso o usuário final marque a caixa de seleção Mostrar log do Windows Installer nas caixas de diálogo SetupCompleteSuccess, SetupCompleteError ou SetupInterrupted e, em seguida, clique em Concluir. (Funciona somente com o Windows Installer 4.0.)
ISPrint	Imprime o conteúdo de um controle ScrollableText em uma caixa de diálogo. Essa é uma ação .dll personalizada do Windows Installer. O nome do arquivo .dll é SetAllUsers.dll e seu ponto de entrada é PrintScrollableText.

Componente	Descrição
CheckForProductUpdates	Usa o FLEXnet Connect para verificar a existência de atualizações do produto. Essa ação personalizada abre um arquivo executável chamado Agent.exe, que transmite o seguinte: /au[ProductCode] /EndOfInstall
CheckForProductUpdatesOnReboot	Usa o FLEXnet Connect para verificar a existência de atualizações do produto ao reinicializar. Essa ação personalizada abre um arquivo executável chamado Agent.exe, que transmite o seguinte: /au[ProductCode] /EndOfInstall /Reboot

- **Diretórios atualizados -** o processo de instalação instala e atualiza arquivos do CA ARCserve Central Applications nos seguintes diretórios, por padrão:

  `C:\Arquivos de programas\CA\ARCserve Central Applications\BIN`

  É possível instalar o CA ARCserve Central Applications no diretório de instalação padrão ou em um diretório diferente. O processo de instalação copia vários arquivos de sistema para o seguinte diretório:

  `C:\WINDOWS\SYSTEM32`

- **Chaves de registro do Windows atualizadas--**o processo de instalação atualiza as chaves de registro do Windows a seguir:

  Chaves padrão do Registro:

  `HKLM\SOFTWARE\CA\CA ARCserve Central Applications`

  O processo de instalação cria chaves de registro e modifica várias outras chaves de registro, de acordo a configuração atual do sistema.

- **Aplicativos instalados**--o processo de instalação inclui estes aplicativos em seu computador:

  – Licenciamento CA
  – Microsoft Visual C++ 2005 SP1 redistribuível
  – Microsoft Windows Installer 3.1 Redistributable (v2) Package
  – JRE (Java Runtime Environment) 1.6.0_16
  – Tomcat 6.0.32

Arquivos binários contendo informações incorretas sobre a versão do arquivo

O CA ARCserve Central Applications instala arquivos binários desenvolvidos por terceiros, outros produtos da CA Technologies e o CA ARCserve Central Applications, os quais contém informações incorretas sobre a versão do arquivo. A tabela abaixo descreve tais arquivos binários.

Nome do arquivo binário	Origem
UpdateData.exe	Licença da CA
zlib1.dll	Biblioteca de compactação zlib

Arquivos binários que não contêm um manifesto incorporado

O CA ARCserve Central Applications instala arquivos binários desenvolvidos por terceiros, outros produtos da CA Technologies e o CA ARCserve Central Applications, os quais não contêm um manifesto incorporado nem em texto. A tabela abaixo descreve tais arquivos binários.

Nome do arquivo binário	Origem
BaseLicInst.exe	Licença da CA
UpdateData.exe	Licença da CA
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
WindowsInstaller-KB893803-v2-x86.exe	Microsoft
tomcat6.exe	Tomcat

Arquivos binários cujo nível de privilégio exige acesso de administrador ao manifesto

O CA ARCserve Central Applications instala arquivos binários desenvolvidos por terceiros, outros produtos da CA Technologies e o CA ARCserve Central Applications com um nível de privilégio de administrador ou o mais alto disponível. É preciso efetuar logon usando uma conta administrativa ou uma conta com o nível de permissão mais alto disponível para executar diversos serviços, componentes e aplicativos do CA ARCserve Central Applications. Os binários correspondentes contêm funcionalidades específicas do CA ARCserve Central Applications, não disponíveis para uma conta de usuário básica. Assim, o Windows solicitará que você confirme uma operação especificando sua senha ou usando uma conta com privilégios administrativos para concluí-la.

- **Privilégios administrativos** - o perfil administrativo ou uma conta com privilégios administrativos têm permissões de leitura, gravação e execução para todos os recursos do Windows e do sistema. Caso não tenha privilégios administrativos, você será solicitado a digitar o nome de usuário e a senha de um usuário administrador para continuar.
- **Privilégios mais altos disponíveis** - uma conta com os privilégios mais altos disponíveis é uma conta de usuário básica e uma conta de usuário avançado que opera com privilégios administrativos.

A tabela abaixo descreve tais arquivos binários.

Nome do arquivo binário	Origem
APMSetupUtility.exe	CA ARCserve Central Applications
ArcAppUpdateManager.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsPMConfigSettings.exe	CA ARCserve Central Applications
CCIConfigSettings.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
D2DAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
D2DPMConfigSettings.exe	CA ARCserve Central Applications
D2DUpdateManager.exe	CA ARCserve Central Applications
DBConfig.exe	CA ARCserve Central Applications
FWConfig.exe	CA ARCserve Central Applications
RemoteDeploy.exe	CA ARCserve Central Applications

Nome do arquivo binário	Origem
RestartHost.exe	CA ARCserve Central Applications
SetupComm.exe	CA ARCserve Central Applications
SetupFW.exe	CA ARCserve Central Applications
SetupWrapper.exe	CA ARCserve Central Applications
Uninstall.exe	CA ARCserve Central Applications
UpdateInstallCommander.exe	CA ARCserve Central Applications
UpgradeDataSyncupUtility.exe	CA ARCserve Central Applications
jbroker.exe	Java Runtime Environment
jucheck.exe	Java Runtime Environment

Capítulo 3: Introdução ao Gerenciador do CA ARCserve Central Protection

As seções a seguir descrevem como configurar o Gerenciador do CA ARCserve Central Protection para proteger os nós do CA ARCserve D2D.

Esta seção contém os seguintes tópicos:

Certifique-se de que o servidor do Gerenciador do CA ARCserve Central Protection possa se comunicar com os nós

Observação: esta é uma etapa opcional para configurar o Gerenciador do CA ARCserve Central Protection para proteger os nós.

Para que o Gerenciador do CA ARCserve Central Protection possa implantar diretivas nos nós e protegê-los, é necessário verificar se o servidor do CA ARCserve Central Protection Manager e os nós que deseja proteger podem se comunicar uns com os outros usando seus nomes de host.

Verifique se o servidor do Gerenciador do CA ARCserve Central Protection pode se comunicar com os nós

1. No servidor do Gerenciador do CA ARCserve Central Protection, execute o comando ping nos nós que deseja proteger usando seus respectivos nomes de host.
2. Nos nós que deseja proteger, execute o comando ping no servidor do Gerenciador do CA ARCserve Central Protection usando seu nome de host.

Configurar programações de sincronização de dados do CA ARCserve Backup

A sincronização de dados do CA ARCserve Backup permite configurar o sistema para definir uma hora programada e método de repetição de quantos dias, qual dia da semana ou do mês que o usuário poderá sincronizar o banco de dados do CA ARCserve Backup com o banco de dados do Gerenciador do CA ARCserve Central Protection.

Siga estas etapas:

1. Efetue logon no aplicativo.
2. Clique em Configuração na barra de navegação para abrir a tela Configuração.
3. No painel Configuração, clique em Programação de sincronização de dados do CA ARCserve Backup para exibir as opções de Sincronização de dados do CA ARCserve Backup.
4. Clique em Ativar para ativar a Sincronização de dados do CA ARCserve Backup.

   Observação: por padrão, a Configuração de sincronização de dados do CA ARCserve Backup está ativada.
5. Especifique os seguintes parâmetros para programar a Sincronização de dados do CA ARCserve Backup:
   - Método de repetição
   - Hora programada
6. Clique em Salvar para aplicar a Programação de sincronização de dados do CA ARCserve Backup.
7. (Opcional) Clique em Executar agora para iniciar o processo de sincronização de dados do CA ARCserve Backup agora.

Configurar programações de SRM

O Gerenciador do CA ARCserve Central Protection permite que administradores de backup configurem uma programação para os nós do CA ARCserve D2D que define quando e com que frequência coletar dados de SRM. SRM (Storage Resource Management) é a funcionalidade que coleta informações sobre o seguinte:

- Hardware, software e dados do aplicativo para implementações do Microsoft SQL Server e do Microsoft Exchange Server.
- Os dados de PKI (Performance Key Indicators - Principais Indicadores de Desempenho) dos servidores do CA ARCserve D2D que são gerenciados por um servidor do CA ARCserve Central Applications.

  Observação: para nós do CA ARCserve Backup, o CA ARCserve Backup coleta dados de PKI e, em seguida, sincroniza os dados com o Gerenciador do CA ARCserve Central Protection durante o processo de sincronização de dados do CA ARCserve Backup.

Siga estas etapas:

1. Efetue logon no aplicativo.
2. Abra a tela Configuração, clicando em Configuração na barra de navegação.
3. No painel Configuração, clique em Configuração de SRM para exibir as opções de configuração de SRM.
4. Clique em Ativar para ativar SRM.

   Observação: por padrão, a Configuração de SRM está ativada.
5. Especifique os seguintes parâmetros para programar o SRM:
   - Método de repetição
   - Hora programada
6. Clique em Salvar para aplicar a programação de SRM.
7. (Opcional) Clique em Executar agora para iniciar o processo de coleta de dados do SRM agora.

Configurar programações de detecção

É possível configurar a programação de detecção para nós de forma repetitiva e em um horário programado. Por padrão, a Configuração da detecção está desativada. Para ativar a configuração, clique na opção Ativar para especificar o tipo de método de repetição desejado e um horário programado para que a detecção do nó se inicie. É possível especificar os seguintes parâmetros para configurar a programação de detecção:

- **Cada quantidade de dias -** permite repetir este método pelo número de dias especificado. (Padrão)
- **Cada dia selecionado da semana -** permite repetir este método nos dias especificados. Segunda-feira, Terça-feira, Quarta-feira, Quinta-feira e Sexta-feira são o padrão para os dias da semana.
- **Cada dia selecionado do mês -** permite repetir este método no dia especificado do mês. 1 é a opção padrão para o dia do mês.

Uma lista do Active Directory é exibida para que você possa visualizar ao configurar uma programação para detectar nós.

Definir configuração de email e alerta

É possível especificar configurações de email e alerta para uso com seu aplicativo, de modo a enviar automaticamente alertas sob as condições determinadas.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, clique em Configuração para abrir a tela Configuração.

2. No painel Configuração, clique em Configuração de email e alerta para abrir as opções de Configuração de email e alerta.

3. Preencha os seguintes campos:
   - **Serviço** - especifique o tipo de serviço de email na lista suspensa. (Google Mail, Yahoo Mail, Live Mail ou Outro).
   - **Servidor de email**--especifique o nome do host do servidor SMTP que o CA ARCserve Central Applications deve usar para enviar email.
   - **Requer autenticação**-selecione essa opção quando o servidor de email especificado exigir autenticação. O nome da conta e a senha serão necessários.
   - **Assunto**--especifique um assunto de email padrão.
   - **De**--especifique o endereço de email para o qual o email está sendo enviado.
   - **Destinatário**--especifique um ou mais endereços de email, separados por um ponto e vírgula (;), para os quais o email será enviado.
   - **Usar SSL** - selecione essa opção se o servidor de email especificado exigir uma conexão segura (SSL).
   - **Enviar STARTTLS** - selecione essa opção se o servidor de email especificado exigir o comando STARTTLS.
   - **Usar formato HTML** - permite enviar mensagens de email no formato HTML. (selecionado por padrão)
   - **Ativar configurações de proxy** - selecione essa opção se houver um servidor proxy. Em seguida, especifique as configurações do servidor proxy.
4. Clique em Testar email para verificar se as definições das configurações de email estão corretas.
5. (Opcional) Na seção Enviar alertas por email, clique nos nós detectados para permitir que o aplicativo envie mensagens de alerta por email quando novos nós forem detectados.
6. Clique em Salvar.

   Observação: você pode clicar em Redefinir para reverter aos valores salvos anteriormente ou clicar em Excluir para excluir as configurações salvas. Excluir as configurações de email e alerta evita que você receba mensagens de alerta por email.

A configuração de email é aplicada.

Configurar as definições do servidor de Gerenciamento de TI

O Gerenciador do CA ARCserve Central Protection permite enviar mensagens de alerta aos servidores de gerenciamento de TI. Para enviar as informações de alerta, configure o servidor do aplicativo para se comunicar com o servidor de gerenciamento de TI.

Para configurar as definições do servidor de gerenciamento de TI

1. Faça logon no CA ARCserve Central Protection Manager e clique em Configuração, em Navegação.
2. Na tela Configuração, clique na opção Configuração do servidor de gerenciamento de TI na lista de configurações.
3. Faça as seguintes opções de configuração do servidor de gerenciamento de TI:
   - Clique em Ativar.
   - Clique em Nimsoft ou Kaseya.
   - Especifique um método de repetição. O método de repetição define os dias da semana para o reenvio das notificações de alerta para o servidor de gerenciamento de TI quando o processo de envio original falhar. O processo de envio de alertas pode falhar quando o servidor de gerenciamento de TI estiver offline ou indisponível.
   - Especifique um cronograma. O cronograma define a hora do dia para enviar novamente as notificações de alerta para o servidor do Nimsoft.
4. Clique em Salvar.

O servidor do Gerenciador do CA ARCserve Central Protection é configurado para se comunicar com o servidor de gerenciamento de TI.

Observação: clique em Redefinir para reverter aos valores salvos anteriormente.

Configurar programações de atualização do CA ARCserve Central Applications

O aplicativo permite configurar uma programação para fazer download automaticamente de atualizações do produto de um Servidor da CA ou de um servidor de armazenamento temporário de software local.

Para configurar programações de atualização do CA ARCserve Central Applications

1. Efetue logon no aplicativo.
2. Clique em Configuração na barra de navegação para abrir a tela Configuração.
3. No painel Configuração, clique em Atualizar configuração.

   As opções de configuração de atualização são exibidas.
4. Selecione um servidor de download.
   - **CA Server** - clique em Configurações de proxy para as seguintes opções:
     - **Usar configurações de proxy do navegador -** permite usar as credenciais fornecidas para as configurações de proxy do navegador.

       Observação: a opção Usar configurações de proxy do navegador afeta o Internet Explorer e o Chrome.
     - **Configurar definições de proxy** - especifique o Endereço IP ou o Nome do host do servidor proxy e o número de porta. Se o servidor especificado exigir autenticação, clique em O servidor proxy exige autenticação e forneça as credenciais.

       Clique em OK para voltar à Atualizar configuração.
   - **Servidor de armazenamento temporário -** se você selecionar essa opção, clique em Adicionar Servidor para adicionar um servidor de armazenamento temporário na lista. Digite o nome de host e o número da porta e clique em OK.

     Se forem especificados vários servidores de armazenamento temporário, o aplicativo tentará usar o primeiro servidor da lista. Se a conexão for bem-sucedida, os demais servidores relacionados não são usados para armazenamento temporário.
5. (Opcional) Clique em Testar conexão para verificar a conexão de servidor e aguarde até que o teste seja concluído.
6. (Opcional) Clique em Verificar atualizações automaticamente e especifique o dia e a hora. Você pode especificar uma programação diária ou semanal.

Clique em Salvar para aplicar a configuração atualizada.

Definir configurações de proxy

O CA ARCserve Central Applications permite especificar um servidor proxy para se comunicar com o suporte da CA a fim de verificar e fazer download das atualizações disponíveis. Para ativar este recurso, é necessário especificar o servidor proxy que deseja que se comunique em nome do servidor do CA ARCserve Central Applications.

Siga estas etapas:

1. Efetue logon no aplicativo e clique em Configuração na barra de navegação.

   A opção Configuração é exibida.

2. Clique em Atualizar configuração.

   As opções de configuração de atualização são exibidas.

3. Clique em Configurações de proxy.

   A caixa de diálogo Configurações de proxy é aberta.

4. Clique em uma das seguintes opções:

   ■ **Usar configurações de proxy do navegador --**permite que o aplicativo detecte e use as mesmas configurações de proxy que são aplicadas para o navegador para se conectar ao servidor da CA Technologies para atualizar as informações.

     Observação: esse comportamento se aplica somente aos navegadores Internet Explorer e Chrome.

   ■ **Definir configurações de proxy**--permite definir um servidor alternativo que o aplicativo usará para se comunicar com o suporte da CA para verificar se há atualizações. O servidor alternativo (proxy) pode ajudar a garantir a segurança, melhorar o desempenho e garantir o controle administrativo.

     Preencha os seguintes campos:

     – **Servidor proxy--** especifique o nome do host ou o endereço IP do servidor proxy.

     – **Porta--**especifique o número de porta que o servidor proxy usará para se comunicar com o site de suporte da CA.

     – **(Opcional) o servidor proxy requer autenticação--** se as credenciais de logon do servidor proxy não forem as mesmas do CA ARCserve Central Applications, clique na caixa de seleção próxima ao Servidor proxy requer autenticação, e especifique o nome de usuário e a senha necessárias para efetuar logon no servidor proxy.

       Observação: use o seguinte formato para especificar o nome de usuário: <nome de domínio>/<nome de usuário>.

   Clique em OK.

As configurações de proxy são definidas

Configurando preferências de redes sociais

O CA ARCserve Central Applications permite gerenciar as ferramentas de rede social para ajudá-lo a gerenciar o aplicativo. Você pode gerar novos feeds, especificar links para sites de redes sociais populares e selecionar sites de fonte de vídeos.

Para configurar preferências de redes sociais

1. Efetue logon no aplicativo.

   Na Barra de navegação na página inicial, clique em Configuração.

   A tela Configuração é exibida.

2. No painel Configuração, clique em Configuração de preferências.

   A opção Preferências é exibida.

3. Especifique as opções necessárias:

   - **Feed de notícias -** permite que o aplicativo exiba feeds RSS de notícias relacionadas ao CA ARCserve Central Applications e ao CA ARCserve D2D e informações do produto (do Expert Advice Center). Os feeds são exibidos na página inicial.
   - **Rede social -** permite que o aplicativo exiba ícones na página inicial para acesso ao Twitter e ao Facebook para sites de redes sociais relacionados ao CA ARCserve Central Applications e ao CA ARCserve D2D .
   - **Vídeos -** permite selecionar o tipo de vídeo para exibição dos produtos do CA ARCserve Central Applications e CA ARCserve D2D. (A opção padrão é Usar vídeos do YouTube.)

   Clique em Salvar.

   As opções de Rede social são aplicadas

4. Na barra de navegação, clique em Página Inicial.

   A Página inicial é exibida.

5. Atualize a janela do navegador.

   As opções de Rede social são aplicadas.

Modificar a conta do administrador

O CA ARCserve Central Applications permite modificar o nome de usuário, senha, ou ambos da conta do administrador depois de instalar o aplicativo. Esta conta de administrador somente é usada para exibição do nome de usuário padrão na tela de logon.

Observação: o nome de usuário especificado deve ser uma conta administrativa do Windows ou uma conta que tenha privilégios administrativos do Windows.

Siga estas etapas:

1. Efetue logon no aplicativo e clique em Configuração na barra de navegação.

   A opção Configuração é exibida.

2. Clique em Conta de administrador

3. A configuração da conta do administrador é exibida.

4. Atualize os seguintes campos, conforme necessário:

   - Nome de usuário
   - Senha

   Clique em Salvar

A conta do administrador é modificada.

Especificar configurações padrão de implantação do D2D

O Gerenciador do CA ARCserve Central Protection permite especificar configurações de implantação do D2D em relação ao local em que o CA ARCserve D2D será implantado.

Observação: para implantar o CA ARCserve D2D em computadores que executam o Windows XP, desative a opção Usar compartilhamento simples de arquivo no computador remoto com Windows XP.

Para especificar configurações de implantação do D2D

1. Efetue logon no aplicativo.

   Na Barra de navegação na página inicial, clique em Configuração.

   A tela Configuração é exibida.

2. No painel Configuração, clique em Configuração de implantação do D2D.

   As opções de Configuração de implantação do D2D são exibidas.

3. Preencha os seguintes campos na tela de configuração:
   - **Porta**--este número de porta é usado para conexão com a interface web do usuário. Por padrão, o número da porta é 8014.
   - **Caminho de instalação**--esse é o caminho de instalação no servidor remoto para o CA ARCserve D2D. Por padrão, o local é %Arquivos de Programas%.
   - **Permitir que o programa de instalação instale o driver** (selecionada por padrão)--especifique se desejar que o programa de instalação instale o driver automaticamente.
   - **Reiniciar** (o padrão é Sim)--especifique se deseja que a reinicialização exigida seja feita automaticamente após a conclusão do processo de implantação ou se deseja executá-la manualmente mais tarde.
   - **Usar HTTPS** (o padrão é Não)--o HTTPS (seguro) fornece um nível superior de segurança que a comunicação HTTP. O HTTPS é o protocolo de comunicação recomendado se você transmite informações confidenciais pela rede.
4. Clique em Salvar.

A opção Implantar a configuração do D2D é aplicada.

Configurar o banco de dados

Depois de instalar o Gerenciador do CA ARCserve Central Protection, é possível fazer o seguinte:

- Atualizar as configurações para o banco de dados do Gerenciador do CA ARCserve Central Protection. Por exemplo, é possível atualizar o nome de instância, os valores de porta, e assim por diante.
- Alterar o aplicativo de banco de dados do Gerenciador do CA ARCserve Central Protection para o Microsoft SQL Server.
- Alterar o aplicativo de banco de dados do Gerenciador do CA ARCserve Central Protection para o Microsoft SQL Server Express Edition.

Para configurar o banco de dados do Gerenciador do CA ARCserve Central Protection

1. Na barra de navegação, clique em Configuração.
2. No Painel de configuração, clique em Configuração do banco de dados.
3. Preencha os seguintes campos na tela de configuração:
   - **Nome da máquina do SQL Server** - especifique o nome do servidor que hospeda a instância do SQL Server.
   - **Instância do SQL Server** - especifique o nome da instância do SQL Server.
   - **Porta do SQL Server -** especifique o número da porta para esta instância ou ative a opção de Detecção automática.
   - **Escolha o modo de autenticação** - o Modo de autenticação do Windows é a seleção padrão.

     Observação: a seleção de SQL Server e Modo de autenticação do Windows ativa os campos Nome de usuário e Senha.
   - (Opcional) **teste -** clique em Testar para verificar se o aplicativo pode se comunicar com a instância do Microsoft SQL Server.
   - **Especifique os valores de Pool de conexões de banco de dados -** para Conexões máximas e mínimas, digite um valor entre 1 e 99.
4. Clique em Salvar.

   Observação: clique em Redefinir para limpar todos os valores especificados e carregar os dados originais.
5. (Opcional) Se o aplicativo fornecer dados para o CA ARCserve Central Reporting, abra o Gerenciador do servidor Windows e reinicie o seguinte serviço:

   ```
   Serviço do CA ARCserve Central Applications
   ```

   A configuração do servidor de banco de dados é aplicada.

Recrie o banco de dados do Gerenciador do CA ARCserve Central Protection

Por vários motivos, você pode desejar recriar o banco de dados do Gerenciador do CA ARCserve Central Protection. Por exemplo, o banco de dados atual consome mais que 10 GB de dados. O procedimento a seguir descreve como recriar o banco de dados do Gerenciador do CA ARCserve Central Protection. Ele se aplica aos bancos de dados do Microsoft SQL Server e Microsoft SQL Server Express Edition.

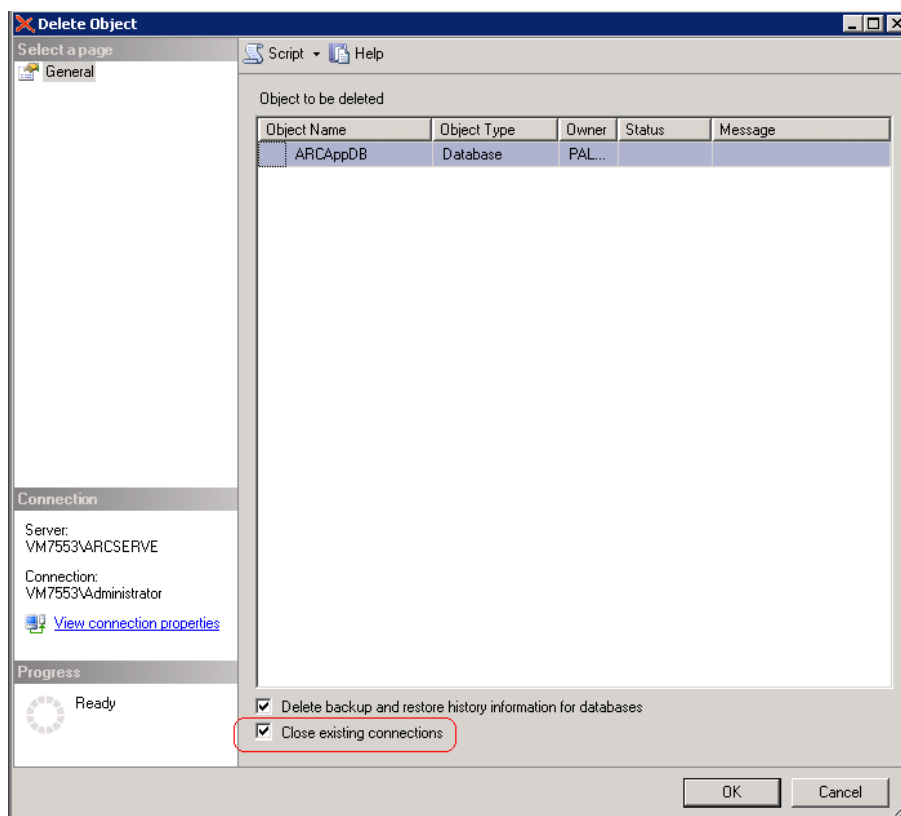
Importante! Ao excluir o banco de dados do Gerenciador do CA ARCserve Central Protection, todos os dados serão perdidos.

Para recriar o banco de dados do Gerenciador do CA ARCserve Central Protection

1. Abra o Microsoft SQL Server Management Studio Express e efetue logon na instância do ARCserve_APP.

   Observação: se o Microsoft SQL Server Management Studio Express não estiver instalado no servidor do Gerenciador do CA ARCserve Central Protection, é possível fazer download do utilitário do Centro de Download da Microsoft.

2. Clique com o botão direito do mouse em ARCAppDB e clique em Excluir no menu pop-up.

   A caixa de diálogo Excluir objeto é exibida.

3. Na caixa de diálogo Excluir objeto, clique nas opções Fechar conexões existentes e clique em OK.

   A caixa de diálogo Excluir objeto é fechada e o banco de dados do Gerenciador do CA ARCserve Central Protection é excluído.

4. Abra o Gerenciador do CA ARCserve Central Protection e clique em Configuração na barra de navegação.

   As opções de configuração são exibidas.

5. Clique em Configuração do banco de dados.

   As opções do banco de dados são exibidas.

6. Verifique se os valores especificados nos campos a seguir estão corretos:
   - **Nome da máquina do SQL Server** - especifique o nome do servidor que hospeda a instância do SQL Server.
   - **Instância do SQL Server** - especifique o nome da instância do SQL Server.
7. (Opcional) Preencha os seguintes campos:
   - **Porta do SQL Server -** especifique o número da porta para esta instância ou ative a opção de Detecção automática.
   - **Escolha o modo de autenticação** - o Modo de autenticação do Windows é a seleção padrão.

     Observação: a seleção de SQL Server e Modo de autenticação do Windows ativa os campos Nome de usuário e Senha.
   - **Especifique os valores de Pool de conexões de banco de dados -** para Conexões máximas e mínimas, digite um valor entre 1 e 99.
8. Clique em Teste para estabelecer uma conexão com o banco de dados.
9. Clique em Salvar.

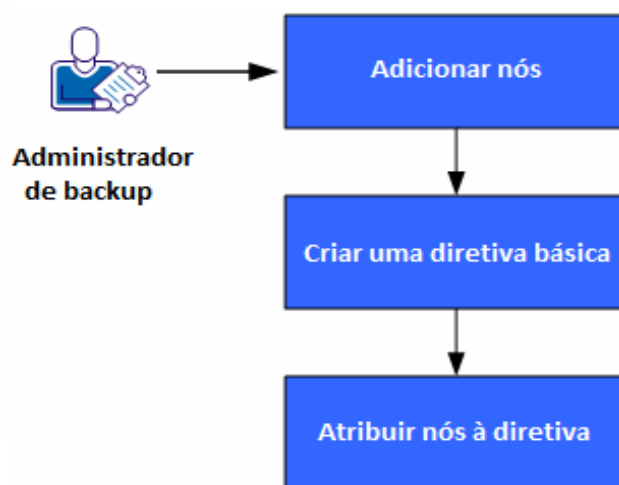
O Gerenciador do CA ARCserve Central Protection recria o banco de dados. O nome da instância do banco de dados é ARCAppDB.

Capítulo 4: Usando o Gerenciador do CA ARCserve Central Protection

Esta seção contém os seguintes tópicos:

Usando o Gerenciador do CA ARCserve Central Protection para fazer backup dos nós do CA ARCserve D2D

Usando o Gerenciador do CA ARCserve Central Protection, é possível criar diretivas que definem como e quando fazer backup e armazenar os dados que residem em nós do CA ARCserve D2D. As informações contidas nos tópicos a seguir descrevem como enviar tarefas de backup do CA ARCserve D2D usando uma diretiva básica. As diretivas básicas podem proteger a maioria dos nós do CA ARCserve D2D que funcionam em ambientes de produção.

O diagrama a seguir ilustra o processo de uso do Gerenciador do CA ARCserve Central Protection para criar uma diretiva de backup básica e fazer backup dos nós do CA ARCserve D2D:

Siga estas etapas para usar o Gerenciador do CA ARCserve Central Protection para criar uma diretiva básica e fazer backup dos nós do CA ARCserve D2D:

1. Adicionar nós (na página 47).
2. Criar uma diretiva básica (na página 47).
3. Atribuir nós à diretiva (na página 52).

Adicionar nós

Para fazer backup dos nós do CA ARCserve D2D usando uma diretiva, defina primeiro os nós para backup.

Observação: você pode usar a opção Detectar para automatizar essa tarefa. No entanto, a opção Detectar detecta somente os nós exibidos no Active Directory em servidores do Active Directory.

Siga estas etapas:

1. Efetue logon no Gerenciador do CA ARCserve Central Protection e clique em Nó na barra de navegação.
2. Na barra de ferramentas Nó, clique em Adicionar e, em seguida, clique em Adicionar nó por IP/nome no menu pop-up.
3. Preencha todos os campos na caixa de diálogo Adicionar nó por IP/nome e clique em OK.
4. (Opcional) Se o nó recém-adicionado não aparecer na lista de nós, clique em Atualizar na barra de ferramentas Nó.

   Observação: para adicionar mais nós, repita as etapas 2, 3 e 4.

Após ser adicionado, o nó é exibido nos grupos padrão.

Criar uma diretiva básica

As diretivas definem como e quando fazer backup e armazenar os dados que residem em nós do CA ARCserve D2D. O Gerenciador do CA ARCserve Central Protection não contém diretivas padrão. Criar uma diretiva é uma tarefa de pré-requisito para fazer backup dos dados que residem nos nós.

Para criar uma diretiva básica, especifique as configurações de proteção e crie uma programação. As configurações de proteção definem os dados para backup, onde e como armazenar os dados. A programação define quando e com que frequência fazer o backup dos nós.

Siga estas etapas:

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação para abrir a tela Diretivas.
2. Clique em Novo para criar uma diretiva.
3. No campo Nome da diretiva na caixa de diálogo Nova diretiva, especifique um nome para a diretiva.
4. Clique na guia Configurações de backup e, em seguida, clique em Configurações de proteção para exibir as opções de Configurações de proteção.

5. Especificar o destino do backup.

   É possível especificar um caminho local (volume ou pasta) ou uma pasta compartilhada remota (ou unidade mapeada) para o local do backup.

   - Se você especificar a execução do backup em seu caminho local (volume ou pasta), o destino de backup especificado não pode ser o mesmo local da origem. Se a origem for incluída no destino por engano, a tarefa irá ignorar essa parte da origem e não a incluirá no backup.

     Importante: Verifique se o volume de destino especificado não contém informações do sistema. O CA ARCserve D2D não faz backup de volumes de destino que contiverem informações do sistema. Ao tentar recuperar o computador usando a BMR (Bare Metal Recovery - Recuperação Bare Metal), a recuperação poderá falhar.

     Observação: discos dinâmicos não podem ser restaurados no nível do disco. Se o backup dos dados for feito no volume de um disco dinâmico, você não poderá restaurar este disco durante a BMR.

   - Ao fazer o backup de dados em um local compartilhado e remoto, especifique um caminho do local e as credenciais necessárias para acessar o computador remoto.

6. Especificar a origem do backup.

   Você pode especificar o backup do nó inteiro ou de um volume individual no nó.

   Esteja ciente do seguinte:

   - Se a opção de backup completo do computador for selecionada, o CA ARCserve D2D detectará automaticamente todos os discos e volumes acoplados ao computador atual e os incluirá no backup.

   - Se o volume de sistema/inicialização não estiver selecionado para backup, uma mensagem de aviso é exibida. A mensagem indica que o backup não pode ser usado para a BMR.

7. Especificar os pontos de recuperação.

   Especifica a quantidade de imagens de backup retidas. O padrão é de 31 e o máximo é 1344. Ao modificar essa quantidade, considere a quantidade de espaço livre disponível no destino.

   Quando a quantidade de pontos de recuperação especificada é excedida, o CA ARCserve D2D mescla o backup incremental filho mais antigo com o backup pai e recria a imagem de linha de base. A nova imagem de linha de base consiste nos blocos de pai e filho mais antigo. O ciclo de mesclagem do backup filho mais antigo com o backup pai se repete para cada backup subsequente. Esse processo permite executar backups incrementais ininterruptamente, enquanto mantém a mesma contagem de retenção.

8. Especifique o tipo de compactação que deseja usar para os backups.

   A compactação reduz o uso de espaço em disco, mas também tem um impacto inverso sobre a velocidade do backup, devido ao aumento no uso da CPU.

   As opções de compactação disponíveis são as seguintes:

   Nenhuma compactação

   Nenhuma compactação será executada. Essa opção exige menos uso da CPU (mais velocidade), mas também mais uso de espaço em disco para a imagem de backup.

   Compactação padrão

   Alguma compactação será realizada. Essa opção proporciona um bom equilíbrio entre o uso da CPU e o uso do espaço em disco. Compactação padrão é a configuração padrão.

   Compactação máxima

   A compactação máxima será realizada. Essa opção proporciona maior uso da CPU (menos velocidade), mas também menos uso de espaço em disco para a imagem de backup.

   Esteja ciente do seguinte:

   - Se a imagem de backup contiver dados não compactáveis (como imagens JPG, arquivos ZIP, etc.), aloque espaço de armazenamento para lidar com esses dados.
   - Se o destino não tiver espaço livre suficiente, considere aumentar a configuração de compactação do backup.

9. Especifique as configurações de criptografia que deseja usar para aumentar a segurança.

   a. Selecione o tipo de algoritmo de criptografia que deseja usar para os backups.

      A criptografia de dados é a conversão de dados em uma forma ininteligível sem um mecanismo decodificador. A proteção de dados do CA ARCserve D2D usa algoritmos de criptografia seguros AES (padrão de criptografia avançada) para atingir o máximo de segurança e privacidade dos dados especificados.

      As opções de formatação são Sem criptografia, AES-128, AES-192 e AES-256. (Para desativar criptografia, selecione Sem criptografia.)

      - Um backup completo e todos os seus respectivos backups incrementais e de verificação deverão usar o mesmo algoritmo de criptografia.
      - Ao alterar o algoritmo de criptografia para um backup incremental ou um backup de verificação, execute um backup completo. Isso significa que, após a alteração de algoritmo de criptografia, o primeiro backup será completo, independentemente do tipo de backup original.

        Por exemplo, se você alterar o formato do algoritmo e enviar um backup personalizado incremental ou de verificação manualmente, ele é convertido automaticamente para um backup completo.

b. Após especificar um algoritmo de criptografia, você deve fornecer (e confirmar) uma senha de criptografia.

   - A senha de criptografia é limitada a um máximo de 23 caracteres.
   - Um backup completo e todos os seus respectivos backups incremental e de verificação devem usar a mesma senha para criptografar dados.
   - Se você alterar a senha de criptografia para um backup incremental ou um backup de verificação, execute um backup completo. Isso significa que, após a alteração de senha de criptografia, o primeiro backup será completo, independentemente do tipo de backup.

     Por exemplo, se você alterar a senha de criptografia e enviar um backup personalizado incremental ou de verificação manualmente, ele será convertido automaticamente para um backup completo.

Quando a criptografia está ativada, o log de atividades é atualizado para descrever a criptografia usada para cada backup.

10. Especifique o Acelerador de backup.

    Você pode especificar a velocidade máxima (MB/min) em que os backups são gravados. Você pode restringir a velocidade de backup para reduzir a utilização da CPU ou da rede. No entanto, limitar a velocidade de backup afeta negativamente a janela de backup.

11. Clique na guia Programar para exibir as opções de Programar.

12. Especifique a programação de backup:

    Definir data e hora de início

    Especifica a data de início e hora de início para seus backups programados.

    Backup incremental

    Especifica a programação de backups para backups incrementais.

    As opções disponíveis são Repetir e Nunca. Se selecionar a opção Repetir, especifique o tempo decorrido (em minutos, horas ou dias) entre as tentativas de backup. A configuração mínima para os backups incrementais é a cada 15 minutos.

    Por padrão, os backups incrementais são programados para serem repetidos uma vez por dia.

Backup completo

Especifica a programação de backups para backups completos.

Conforme programado, o CA ARCserve D2D executará um backup completo de todos os blocos do computador de origem. As opções disponíveis são Repetir e Nunca. Se selecionar a opção Repetir, especifique o tempo decorrido (em minutos, horas ou dias) entre as tentativas de backup. A configuração mínima para os backups completos é a cada 15 minutos.

Por padrão, a programação para backups completos é Nunca (nenhuma repetição programada).

Backup de verificação

Especifica a programação de backups para backups de verificação.

As opções disponíveis são Repetir e Nunca. Se selecionar a opção Repetir, especifique o tempo decorrido (em minutos, horas ou dias) entre as tentativas de backup. A configuração mínima para os backups de verificação é a cada 15 minutos.

Por padrão, a programação para backups de verificação é Nunca (nenhuma repetição programada).

13. Clique em Salvar.

A diretiva de backup básica é criada. A diretiva é exibida na lista de diretivas, com o nome que você especificou na etapa 3 na tela Diretivas.

Observação: se em um determinado momento houver mais de um tipo de backup programado para execução simultânea, o tipo de backup que será executado terá como base as seguintes prioridades:

- Prioridade 1 - Backup completo
- Prioridade 2 - Backup de verificação
- Prioridade 3 - Backup incremental

Exemplo: quando todos os três tipos de backup estiverem programados para executar simultaneamente, o CA ARCserve D2D executará o backup completo. O CA ARCserve D2D executará backups de verificação quando backups de verificação e backups incrementais estiverem programados para executar simultaneamente e não houver nenhum backup completo programado. Um backup incremental programado só será executado se não houver conflito com nenhum outro tipo de backup.

Atribuir nós à diretiva

Depois de criar a diretiva básica, atribua os nós do CA ARCserve D2D para backup usando a diretiva.

Siga estas etapas:

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação para abrir a tela Diretivas.
2. Na lista de diretivas na tela Diretivas, clique na diretiva que você criou.
3. Clique na guia Atribuição de diretiva para exibir a (lista de) atribuição de diretiva.
4. Clique em Atribuir e remover atribuição para abrir a caixa de diálogo Atribuir/Remover atribuição de diretiva.
5. Clique na caixa de seleção ao lado do nó ou nós que deseja adicionar e clique na seta à direita.

   A caixa de diálogo do Contrato de licença será exibida.
6. Leia e aceite os termos do Contrato de Licença e clique em Concluído.

   Os nós serão atribuídos à diretiva criada e implantados imediatamente. Os backups são iniciados com base na programação definida na guia Programar.
7. Quando terminar de atribuir nós a diretivas, clique em OK para salvar as atribuições de diretivas e fechar a caixa de diálogo Atribuir e remover atribuição.

Depois que os nós forem atribuídos, o Gerenciador do CA ARCserve Central Protection implantará a diretiva nos nós imediatamente. As operações de backup são iniciadas com base nas configurações de proteção selecionadas e seguindo a programação definida na diretiva.

Como gerenciar nós no Gerenciador do CA ARCserve Central Protection

O Gerenciador do CA ARCserve Central Protection fornece várias ferramentas e opções que podem ser usadas para gerenciar nós e grupos de nós. Esta seção contém informações sobre como adicionar, excluir, modificar e sincronizar dados para nós e grupos de nós. Também é possível detectar e implantar o CA ARCserve D2D para nós.

Esta seção contém os seguintes tópicos:

Compreendendo a tela Gerenciamento de nós

Gerenciamento de nós é um componente de entrada do CA ARCserve Central Applications. É possível acessá-lo na Barra de navegação no painel esquerdo do aplicativo Gerenciador do CA ARCserve Central Protection.

O Gerenciamento de nós contém quatro categorias para o trabalho na tela:

- **Nó -** permite gerenciar nós específicos. Para obter mais informações sobre o gerenciamento de nós, consulte O que você pode fazer com nós (na página 55).
- **Grupo de nós -** permite gerenciar grupos de nós específicos. Para obter mais informações, consulte o tópico O que você pode fazer com grupos de nós (na página 70).
- **Ações -** permite Fazer backup de dados (na página 135), Restaurar dados (na página 137) e Implantar dados (na página 77).
- **Filtro--**permite usar filtros para exibir nós de um grupo com determinado aplicativo instalado. Para obter mais informações, consulte Filtrar grupos de nós (na página 80).

O status de cada nó localizado na coluna Produtos identifica os ícones do CA ARCserve Backup e CA ARCserve D2D. A tabela a seguir descreve o status de cada produto na coluna Produto:

Ícone	Descrição
	Este status com a letra 'M' indica que o nó é um servidor principal ou autônomo do CA ARCserve Backup gerenciado pelo CA ARCserve Central Applications.
	Este status com a letra 'M' e um ponto de exclamação na parte inferior direita indica que o nó é um servidor principal ou autônomo do CA ARCserve Backup gerenciado pelo CA ARCserve Central Applications sem sincronização bem-sucedida nas últimas 'xx' horas. ('xx' foi definido como 48 horas por padrão) ou a sincronização ainda não foi executada.
	Este status sem a letra 'M' indica que o nó é um servidor principal, autônomo ou membro do CA ARCserve Backup e não gerenciado pelo CA ARCserve Central Applications.
	Este status indica que esse nó contém uma versão mais antiga do CA ARCserve Backup
	Este status indica que o nó não é gerenciado pelo CA ARCserve Central Applications e não se pode conectar ao CA ARCserve D2D.
	Este status indica que o nó contém uma versão mais antiga do CA ARCserve D2D.
	Este status com a letra 'M' indica que o nó é gerenciado pelo CA ARCserve Central Applications e está conectado ao CA ARCserve D2D.
	Este status com a letra 'M' indica que o nó é gerenciado pelo CA ARCserve Central Applications e não se pode conectar ao CA ARCserve D2D.
	Este status com a letra 'M' indica que o nó é gerenciado pelo CA ARCserve Central Applications e está conectado ao CA ARCserve D2D com avisos.
	Este status com a letra 'M' e um ponto de exclamação na parte inferior direita indica que o nó é um servidor do CA ARCserve D2D gerenciado pelo CA ARCserve Central Applications sem sincronização bem-sucedida nas últimas 'xx' horas. ('xx' foi definido como 48 horas por padrão) ou a sincronização ainda não foi executada.

O que você pode fazer com nós

O Gerenciador do CA ARCserve Central Protection permite adicionar, modificar e excluir nós, sincronizar dados, especificar configurações de nó, detectar nós, exportar informações de nó para CSV e determinar o status de cada nó.

Observação: ao adicionar nós ao Gerenciador do CA ARCserve Central Protection com servidores correspondentes do CA ARCserve Backup e CA ARCserve D2D e, em seguida, executar uma sincronização em cada nó, os dados deste nó específico são gerados e podem ser exibidos no CA ARCserve Central Reporting. Para obter mais detalhes sobre a sincronização, consulte o tópico Opções e dados da sincronização (na página 66).

Adicionar nós usando a opção Detectar

O Gerenciador do CA ARCserve Central Protection permite adicionar vários nós do processo Detectar.

Para adicionar nós usando a opção Detectar

1. Efetue logon no aplicativo e clique em Nós na barra de navegação.

   A tela Nós é aberta.

2. Clique em Detectar na barra de ferramentas Nó.

   A caixa de diálogo Discover by active directory é exibida.

3. Preencha os seguintes campos:

   - Nome de usuário (domínio)
   - Senha (domínio)
   - Filtragem pelo nome do computador

   Clique em Adicionar e em seguida Iniciar a detecção.

   A opção Detectar (na página 56) é executada.

4. Quando a detecção de nós for concluída, a seguinte mensagem de confirmação será exibida:

   `Deseja continuar a adicionar nós a partir do resultado da detecção?`

   Selecione Sim para ir para Adicionar nós a partir do resultado da detecção.

   Observação: para fechar a mensagem sem adicionar nós, clique em Não.

   A tela Adicionar nós a partir do resultado da detecção é exibida, mostrando uma lista dos nós detectados.

5. Na lista Nós detectados, selecione os nós que deseja adicionar e clique na seta para adicioná-los à lista Nós para proteger. Clique em Avançar ao terminar.

   Observação: é possível filtrar a lista por nome do nó ou domínio para reduzir a lista.

6. (Opcional) Selecione um ou mais nós e clique em Ocultar nós selecionados para ocultar nós que não deseja fazer backup.

7. (Opcional) Verifique a opção Mostrar nós ocultos para exibir nós ocultos novamente na lista Nós detectados. Para ocultar os nós novamente, desmarque a opção.

8. Na tela Credenciais do nó, forneça um nome de usuário e uma senha para o nó que deseja adicionar. É possível especificar credenciais globais ou aplicar credenciais aos nós selecionados.

9. Clique em Concluir.

Os nós são adicionados.

Caixa de diálogo Monitor de detecção

Esta caixa de diálogo exibe o status geral dos nós detectados em seu ambiente.

A caixa de diálogo fornece as seguintes informações:

Fase

Exibe as três fases na detecção de nós: detectando nós, atualizando dados e detecção concluída.

Status

Exibe um status Ativo durante o processo de detecção e, em seguida, exibe o status Concluído quando a detecção for concluída.

Tempo decorrido

Exibe o tempo para detectar os nós.

Quantidade de nós processados

Exibe a contagem de nós processados que estão conectados e atualizados no banco de dados.

Adicionar nós por endereço IP ou nome de nó

O Gerenciador do CA ARCserve Central Protection permite que você adicione nós do CA ARCserve D2D e do CA ARCserve Backup a grupos de nós, consultando o endereço IP ou o nome do host do nó.

Para adicionar nós por endereço IP ou nome de nó

1. Na página inicial, selecione Nó na Barra de navegação.

   A tela Nó é exibida.

2. Na barra de ferramentas Nó, clique em Adicionar e, em seguida, clique em Adicionar nó por IP/nome no menu pop-up.

   A caixa de diálogo Adicionar nó por IP/Nome é aberta.

3. Preencha os campos abaixo na caixa de diálogo Adicionar nó por do IP/Nome:

   - **IP/Nome do nó** - permite especificar o endereço IP ou o nome do nó.
   - **Descrição** - permite especificar uma descrição para o nó.
   - **Nome de usuário -** permite especificar o nome de usuário necessário para efetuar logon no nó.
   - **Senha -** permite especificar a senha necessária para fazer logon no nó.

   Clique em OK.

4. (Opcional) Se o nó recém-adicionado não aparecer na lista de nós, clique em Atualizar na barra de ferramentas Nó.

   A caixa de diálogo Adicionar nó por IP/Nome é fechada e o nó é adicionado.

5. (Opcional) Se o CA ARCserve Backup estiver instalado no nó e as credenciais do Gerenciador do CA ARCserve Central Protection não tiverem privilégios de administrador do CA ARCserve Backup, a seguinte mensagem será exibida:

   ```
   É necessário ter privilégio de administrador no ARCserve Backup.
   ```

   Para continuar, especifique as credenciais de logon para a conta de administrador do CA ARCserve Backup e clique em OK.

   Observação: o Gerenciador do CA ARCserve Central Protection pode executar a sincronização de dados somente em servidores principais e autônomos do CA ARCserve Backup. Quando o servidor principal é um servidor de filial, o Gerenciador do CA ARCserve Central Protection pode sincronizar os dados do CA ARCserve Backup apenas com o servidor do painel global.

O nó é adicionado.

Adicionar nós a partir do resultado da detecção

Esta opção permite selecionar os nós que são detectados automaticamente com base nas configurações especificadas no painel Configuração da detecção.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Clique em Nós na barra de navegação para abrir a tela Nós.

2. Na categoria Nó, clique em Adicionar e, em seguida, clique em Adicionar nós a partir do resultado da detecção no menu pop-up.

   A tela Adicionar nós a partir do resultado da detecção é exibida, mostrando uma lista dos nós detectados.

3. Na lista Nós detectados, selecione os nós que deseja adicionar e clique na seta para adicioná-los à lista Nós para proteger. Clique em Avançar ao terminar.

   Observação: é possível filtrar a lista por nome do nó ou domínio para reduzir a lista.

4. (Opcional) Selecione um ou mais nós e clique em Ocultar nós selecionados para ocultar nós que não deseja fazer backup.

5. (Opcional) Verifique a opção Mostrar nós ocultos para exibir nós ocultos novamente na lista Nós detectados. Para ocultar os nós novamente, desmarque a opção.

6. Na tela Credenciais do nó, forneça um nome de usuário e uma senha para o nó que deseja adicionar. É possível especificar credenciais globais ou aplicar credenciais aos nós selecionados.

7. Clique em Concluir.

Os nós são adicionados.

Adicionar nós importando máquinas virtuais do ESX/VC

A opção Adicionar nó permite localizar e adicionar todas as máquinas virtuais em um host ESX ou vCenter Server especificado.

Observação: máquinas com ferramentas VMware instaladas são as únicas máquinas virtuais que podem ser localizadas.

Para adicionar nós importando máquinas virtuais do ESX/VC

1. Efetue logon no aplicativo e clique em Nós na Barra de navegação.

   A tela Nós é aberta.

2. Na barra de ferramentas Nó, clique em Adicionar e em Importar máquinas virtuais do ESX/VC no menu pop-up.

   A caixa de diálogo Detectar nós é aberta.

3. Preencha os campos a seguir da caixa de diálogo Detectar nós

   - Host do servidor ESX ou vCenter - permite especificar o hipervisor a ser verificado.
   - Nome de usuário
   - Senha
   - Porta
   - Protocolo

   Clique em Conectar.

   O aplicativo verifica o hipervisor.

4. Ao ser concluída a verificação, clique em Avançar.

   A caixa de diálogo Credenciais do nó é aberta.

5. Na caixa de diálogo Credenciais do nó, forneça um nome de usuário global e uma senha para todas as máquinas virtuais detectadas e clique em Aplicar aos selecionados.

6. (Opcional) Clique em uma máquina virtual para inserir as credenciais específicas para a máquina virtual.

7. Clique em Concluir.

As máquinas virtuais selecionadas são adicionadas ao grupo de nós.

Importar nós de um arquivo

O Gerenciador do CA ARCserve Central Protection permite importar vários nós de um arquivo. Você pode importar os nós de um arquivo de texto com valores separados por vírgulas (.txt) ou de uma planilha (.CSV).

Para importar nós de um arquivo

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, selecione Nó.

   A tela Nó é exibida.

2. Na barra de ferramentas Nó, clique em Adicionar e, em seguida, clique em Importar nós do arquivo no menu pop-up.

   A caixa de diálogo Selecionar nós é aberta.

3. Clique em Procurar para especificar o arquivo que contém os nós que você deseja importar.

   Observação: é possível especificar um arquivo de valores separados por vírgula (CSV) ou um arquivo de texto que contenha valores separados por vírgula.

   Clique em Carregar.

   Os nomes de nó e os nomes de usuário correspondentes são exibidos na caixa de diálogo.

4. Clique em Avançar.

   A caixa de diálogo Credenciais do nó será aberta.

   Se os nomes de usuário e as senhas fornecidos estiverem corretos, uma marca de seleção verde será mostrada no campo Verificado. Se os nomes de usuário e as senhas fornecidos não estiverem corretos, um ponto de exclamação vermelho será mostrado no campo Verificado.

5. Siga um destes procedimentos:

   - Para adicionar os nós, verifique se todos os nomes de usuário e senhas estão corretos. Para alterar as credenciais de um determinado nó, clique no campo Nome do nó.

     A caixa de diálogo Validar credenciais é aberta.

     Preencha os campos obrigatórios da caixa de diálogo Validar credenciais e clique em OK.

   - Para aplicar um nome de usuário e senha globais a todos os nós, preencha os campos Nome de usuário e Senha e clique em Aplicar à seleção de.

     O nome de usuário e a senha globais são aplicados a todos os nós.

   Clique em Concluir.

Os nós são adicionados.

Atualizar nós

O Gerenciador do CA ARCserve Central Protection permite atualizar informações sobre nós adicionados anteriormente. Atualize os nós quando as condições a seguir ocorrerem:

- **Todos os nós:**
  - Um novo produto foi instalado no nó após o nó ter sido registrado no Gerenciador do CA ARCserve Central Protection.
  - O nome de usuário ou a senha do nó foi atualizado após o nó ter sido registrado no Gerenciador do CA ARCserve Central Protection.
- **Nós do CA ARCserve Backup:**
  - Um servidor de filial do CA ARCserve Backup foi atualizado para um servidor principal do CA ARCserve Backup.
  - Um servidor principal central do CA ARCserve Backup foi atualizado para um servidor principal do CA ARCserve Backup depois que o servidor principal central foi registrado no Gerenciador do CA ARCserve Central Protection.

  Observação: ao adicionar ou atualizar os nós que funcionam como servidores de filiais do CA ARCserve Backup associados a um servidor principal central, o nome do host do servidor principal central é exibido em dois locais na tela Nó. O primeiro local na tela Nó é o grupo Todos os nós. O nome completo do servidor é exibido no grupo Todos os nós, independentemente da quantidade de caracteres contidos no nome do host do servidor. O segundo local na tela Nó é Grupos do painel global. Quando o nome do host do servidor contiver mais de 15 caracteres, ele será truncado para 15 caracteres em Grupos do painel global.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, selecione Nó.

   A tela Nó é exibida.

2. Na barra Grupos, clique no grupo Todos os nós ou clique no nome de grupo contendo os nós que deseja atualizar.

   Os nós associados ao grupo são exibidos na lista de nós.

3. Clique nos nós que deseja atualizar e, em seguida, clique em Atualizar nó no menu pop-up.

   A caixa de diálogo Atualizar nó é exibida.

   Observação: para atualizar todos os nós no grupo de nós, clique com o botão direito do mouse no nome do grupo de nós e, em seguida, clique em Atualizar nó no menu pop-up.

4. Atualize os detalhes do nó, conforme necessário.

   Observação: para atualizar vários nós na lista de nós, selecione os nós desejados, clique com o botão direito do mouse em qualquer nó e clique em Atualizar nó no menu pop-up. O nome de usuário e a senha são os mesmo para todos os nós selecionados. Por padrão, a opção e o Especificar novas credenciais e a caixa de seleção Assumir controle do nó estão selecionados. É possível especificar um novo nome de usuário e senha para os nós selecionados e é possível forçar este servidor a administrar os nós. Além disso, é possível selecionar Usar credenciais existentes para aplicar o nome de usuário e senha atuais. Os campos são desativados.

5. Clique em OK.

   A caixa de diálogo Atualizar nó é fechada e os nós são atualizados.

   Observação: ao atualizar um ou mais dos campos descritos na etapa anterior, a caixa de diálogo Atualizar nó é aberta para que você possa especificar mais detalhes.

6. (Opcional) Se as informações atualizadas não forem exibidas na lista de nós, clique em Atualizar na barra de ferramentas.

O nó é atualizado.

Excluir nós

O Gerenciador do CA ARCserve Central Protection permite excluir nós de seu ambiente.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Clique em Nó na barra de navegação para abrir a tela Nó.

2. Na barra de Grupos, clique no grupo Todos os nós ou clique no nome de grupo contendo o nó que você deseja excluir.

   Os nós associados ao grupo são exibidos na lista de nós.

3. Selecione um ou mais nós que desejar excluir e, em seguida, clique em Excluir na barra de ferramentas.

   Uma mensagem de confirmação é exibida.

4. Siga um destes procedimentos:

   - Clique em Sim para excluir o nó.

   Clique em Não se não desejar excluir o nó.

Exportar nós para um arquivo

O Gerenciador do CA ARCserve Central Protection permite exportar os nós do Grupo de nós com as informações da credencial para um arquivo CSV.

Para exportar nós para um arquivo

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, selecione Nó.

   A tela Nó é exibida.

2. Selecione um grupo de nós para exportação.

   Os nós do grupo de nós selecionado são exibidos.

3. Clique em Exportar na barra de ferramentas Nó.

   Uma mensagem é exibida o notificando de que o arquivo CSV deverá conter as senhas que serão exibidas em texto sem formatação.

   Clique em Sim para abrir ou salvar o arquivo CSV ou clique em Não para cancelar.

Os nós são exportados para um arquivo CSV.

Fazer logon em Nós do CA ARCserve D2D

Na página inicial do Gerenciador do CA ARCserve Central Protection, é possível efetuar logon nos nós do CA ARCserve D2D.

Para fazer logon em nós do CA ARCserve D2D

1. Abra o aplicativo e clique em Nós na Barra de navegação.

   A tela Nó é exibida.

2. Na lista de Grupos, clique em Todos os nós ou clique no grupo que contém o nó do CA ARCserve D2D nó no qual você deseja fazer logon.

   A lista de nós exibe todos os nós associados com o grupo especificado.

3. Procure e clique no nó que deseja efetuar logon e, em seguida, clique em Efetuar logon no D2D no menu pop-up.

   Observação: se uma nova janela do navegador não for aberta, verifique se as opções de pop-up de seu navegador permitem todos os pop-ups ou pop-ups somente para este site.

Você está conectado ao nó do CA ARCserve D2D.

Observação: a primeira vez que efetuar logon no nó do CA ARCserve D2D, uma página HTML pode se abrir exibindo uma mensagem de aviso. Isso pode ocorrer quando estiver usando o Internet Explorer. Para corrigir esse comportamento, feche o Internet Explorer e repita a etapa 3. Assim, será possível fazer logon no nó do CA ARCserve D2D com êxito.

Atualizar nós e diretivas depois de alterar o nome do host no servidor do CA ARCserve Central Applications

Depois de alterar o nome do host do servidor do Gerenciador do CA ARCserve Central Protection, é possível atualizar os nós e as diretivas aplicadas a eles. É possível executar essas tarefas para manter a relação entre o servidor do Gerenciador do CA ARCserve Central Protection e os nós que este servidor está protegendo. A tabela abaixo descreve os possíveis cenários e a ação corretiva para cada cenário.

Cenário	Ação corretiva
O nó foi adicionado depois que nome do host do servidor do Gerenciador do CA ARCserve Central Protection foi alterado.	Nenhuma ação necessária.
O nó foi adicionado antes que o nome do host do servidor do Gerenciador do CA ARCserve Central Protection foi alterado e uma diretiva não foi aplicada ao nó.	Atualize o nó. Para obter mais informações, consulte Atualizar nós (na página 61).

Cenário	Ação corretiva
O nó foi adicionado antes que o nome do host do servidor do Gerenciador do CA ARCserve Central Protection foi alterado e uma diretiva foi aplicada ao nó.	Aplique a diretiva novamente. Para obter mais informações, consulte Implantar diretivas (na página 133).

Opções da tarefa de mesclagem

O Gerenciador do CA ARCserve Central Protection permite pausar e retomar tarefas de mesclagem para cada nó, a qualquer momento. O processo de pausa e retomada de tarefas de mesclagem não afeta as tarefas em andamento.

Pausar uma tarefa de mesclagem em um nó

O Gerenciador do CA ARCserve Central Protection permite pausar uma tarefa de mesclagem em um nó específico.

Por exemplo, as tarefas de mesclagem podem consumir recursos do sistema e fazer com que tarefas de backup sejam executadas com lentidão. Use a opção de pausa para interromper uma tarefa de mesclagem em andamento de modo que as tarefas de backup em andamento possam ser concluídas com a maior eficiência possível. Após a conclusão dos backups, é, então, possível retomar a tarefa de mesclagem.

Siga estas etapas:

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Nó na barra de navegação para abrir a tela Diretiva.
2. Selecione o grupo de nós que contém os nós com tarefas de mesclagem a serem pausadas.

   Uma lista de nós para o grupo de nós selecionado é exibida.
3. Clique nos nós com as tarefas de mesclagem a serem pausadas. Em seguida, clique com o botão direito do mouse nos nós selecionados e clique em Pausar tarefa de mesclagem no menu pop-up.

   Observação: por padrão, a opção Pausar tarefa de mesclagem está desativada. Quando o nó está executando uma tarefa de mesclagem, conforme indicado na coluna de tarefas, a opção Pausar tarefa de mesclagem é ativada.

A tarefa de mesclagem do nó selecionado é pausada e pode ser verificada na página inicial do CA ARCserve D2D.

Retomar uma tarefa de mesclagem em um nó

O Gerenciador do CA ARCserve Central Protection permite retomar tarefas de mesclagem que foram pausadas para nós específicos.

Siga estas etapas:

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Nó na barra de navegação para abrir a tela Diretiva.
2. Selecione o grupo de nós que contém os nós com tarefas de mesclagem a serem retomadas.

   Uma lista de nós para o grupo de nós selecionado é exibida.
3. Clique nos nós com tarefas de mesclagem pausadas que você agora deseja retomar. Em seguida, clique com o botão direito do mouse nos nós selecionados e clique em Retomar tarefa de mesclagem no menu pop-up.

   Observação: a opção Retomar tarefa de mesclagem é ativada quando uma tarefa de backup não está em execução, e as tarefas de mesclagem estão pausadas.

A tarefa de mesclagem do nó selecionado é retomada e pode ser verificada na página inicial do CA ARCserve D2D.

Opções e dados da sincronização

O Gerenciador do CA ARCserve Central Protection permite sincronizar dados para cada nó mediante a transmissão de informações do servidor principal do CA ARCserve Backup (asdb), CA ARCserve D2D, ou do banco de dados principal central do painel global (central_asdb) ao banco de dados do Gerenciador do CA ARCserve Central Protection (ARCAppDB).

A sincronização dos dados manterá os dados nos diferentes bancos de dados consistentes e atualizados para que o banco de dados central contenha as mesmas informações que os bancos de dados de cada local de filial registrado.

Esta seção contém os seguintes tópicos

Realizar uma sincronização completa de dados do CA ARCserve Backup para determinado nó ou grupo de nós

O Gerenciador do CA ARCserve Central Protection permite executar a sincronização completa de dados do CA ARCserve Backup em determinado nó ou grupo de nós.

Durante o processo de sincronização completa do CA ARCserve Backup, o mecanismo de banco de dados do CA ARCserve Backup é interrompido por alguns minutos. Esse comportamento pode impedir a geração de logs de quaisquer informações de tarefas do CA ARCserve Backup até que o processo de sincronização de banco de dados seja concluído.

Para realizar uma sincronização completa de dados do CA ARCserve Backup para determinado nó ou grupo de nós

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Nó na barra de navegação.

   A tela Nó é exibida.

2. Selecione o grupo de nós que contém o nós que deseja sincronizar.

   Uma lista de nós para o grupo de nós selecionado é exibida.

3. Siga um destes procedimentos:

   - Para um nó específico, selecione o nó do CA ARCserve Backup do lado direito da opção Grupos e clique em Sincronização completa do CA ARCserve Backup no menu pop-up ou no botão Sincronizar dados na barra de ferramentas Nó.
   - Para um grupo de nós, clique com o botão direito do mouse no grupo de nós e clique em Fazer sincronização completa do CA ARCserve Backup no menu pop-up.

O Gerenciador do CA ARCserve Central Protection envia uma sincronização completa de dados do CA ARCserve Backup ao nó ou grupo de nós selecionado.

Realizar uma sincronização incremental de dados do CA ARCserve Backup para determinado nó ou grupo de nós

O Gerenciador do CA ARCserve Central Protection permite executar uma sincronização incremental de dados do CA ARCserve Backup em determinado nó.

Fazer sincronização incremental do CA ARCserve Backup sincroniza dados que foram modificados, excluídos ou adicionados depois que a última sincronização foi executada. Os dados sincronizados são compactados para minimizar o tamanho antes da transmissão.

Para realizar uma sincronização incremental de dados do CA ARCserve Backup para determinado nó ou grupo de nós

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Nó na barra de navegação.

   A tela Nó é exibida.

2. Selecione o grupo de nós que contém o nós que deseja sincronizar.

   Uma lista de nós para o grupo de nós selecionado é exibida.

3. Siga um destes procedimentos:

   - Para um nó específico, selecione o nó do CA ARCserve Backup do lado direito da opção Grupos e clique em Sincronização incremental do CA ARCserve Backup no menu pop-up ou no botão Sincronizar dados na barra de ferramentas Nó.
   - Para um grupo de nós, clique com o botão direito do mouse no grupo de nós e clique em Fazer sincronização incremental do CA ARCserve Backup no menu pop-up.

O Gerenciador do CA ARCserve Central Protection envia uma sincronização incremental de dados do CA ARCserve Backup ao nó ou grupo de nós selecionado.

Realizar uma sincronização completa de dados do CA ARCserve D2D para determinado nó ou grupo de nós

O Gerenciador do CA ARCserve Central Protection permite executar a sincronização completa de dados do CA ARCserve D2D em determinado nó ou grupo de nós.

Para realizar uma sincronização completa de dados do CA ARCserve D2D para determinado nó ou grupo de nós

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Nó na barra de navegação.

   A tela Nó é exibida.

2. Selecione o grupo de nós que contém os nós a serem sincronizados.

   Uma lista de nós para o grupo de nós selecionado é exibida.

3. Siga um destes procedimentos:

   - Para um nó específico, selecione o nó do CA ARCserve D2D do lado direito da opção Grupos e clique em Sincronização completa do CA ARCserve D2D no menu pop-up ou no botão Sincronizar dados na barra de ferramentas Nó.
   - Para um grupo de nós, clique com o botão direito do mouse no grupo de nós e clique em Fazer sincronização completa do CA ARCserve D2D no menu pop-up.

O Gerenciador do CA ARCserve Central Protection envia uma sincronização completa de dados do CA ARCserve D2D ao nó ou grupo de nós selecionado.

Configurações do nó

O Gerenciador do CA ARCserve Central Protection permite configurar um local de programação para cada nó do CA ARCserve Backup ou nó principal central do painel global para executar a sincronização incremental.

Aplicar programações de sincronização de dados do CA ARCserve Backup

A configuração do CA ARCserve Backup permite definir programações personalizados para cada nó do CA ARCserve Backup.

Para aplicar programações de sincronização de dados do CA ARCserve Backup

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Nó na barra de navegação.

   A tela Nó é exibida.

2. Selecione o grupo de nós da lista Grupos com o nó ao qual você deseja aplicar a configuração do CA ARCserve Backup.

   Uma lista de nós para o grupo de nós selecionado é exibida.

3. Selecione o nó para aplicar a configuração e, em seguida, clique em Programação de sincronização de dados do CA ARCserve Backup no menu pop-up.

   A caixa de diálogo Programação de sincronização de dados do CA ARCserve Backup é aberta.

4. Selecione uma das seguintes opções:
   - **Ativar -** permite especificar opções de programação inserindo um método de repetição e um horário agendado:
     - Cada quantidade de dias
     - Cada dia selecionado da semana
     - Cada dia selecionado do mês
   - **Desativar -** com esta opção, nenhuma configuração será aplicada.
   - **Usar global -** permite aplicar as configurações globais configuradas no módulo de configuração do CA ARCserve Backup. Para obter mais detalhes, consulte Programações de sincronização de dados do CA ARCserve Backup.
5. Clique em OK.

As configurações do CA ARCserve Backup são aplicadas.

O que você pode fazer com os Grupos de nó

O Gerenciador do CA ARCserve Central Protection permite que você crie grupos de nós com a capacidade de atribuir nós individuais a cada grupo, modificar e excluir grupos de nós.

Observação: só é possível modificar e excluir os grupos de nós criados.

Adicionar grupos de nós

Os grupos de nós permitem gerenciar um grupo de computadores de origem do CA ARCserve D2D de acordo com características comuns. Por exemplo, é possível definir grupos de nós classificados pelo departamento que eles suportam: contabilidade, marketing, jurídico, recursos humanos e assim por diante.

O aplicativo contém os seguintes grupos de nós:

- **Grupos padrão:**
  - **Todos os nós -** contém todos os nós associados ao aplicativo.
  - **Nós sem um grupo** - contém todos os nós associados ao aplicativo que não estão atribuídos a um grupo de nós.
  - **Nós sem uma diretiva** - contém todos os nós associados ao aplicativo que não possuem uma diretiva atribuída.
  - **Servidor SQL -** contém todos os nós associados ao aplicativo e o Microsoft SQL Server está instalado no nó.
  - **Exchange -** contém todos os nós associados ao aplicativo e o Microsoft Exchange Server está instalado no nó.

  Observação: não é possível modificar ou excluir os grupos de nós padrão.
- **Grupos personalizados--**contém grupos de nós personalizados.
- **Grupos de vCenter/ESX**-- ao adicionar um nó a partir da opção Importar máquinas virtuais do vCenter/ESX, o nome do servidor de ESX/vCenter será adicionado a este grupo.
- **Grupos do painel global -** contém todos os nós associados ao servidor principal central.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, clique em Nó para abrir a tela Nó.
2. Clique em Adicionar na barra de ferramentas Grupo de nós.

   A caixa de diálogo Adicionar grupo é aberta e nós aparecem na lista de Nós disponíveis.
3. Especifique um nome de grupo para o grupo de nós.

4. Preencha os campos abaixo na caixa de diálogo Adicionar grupo:
   - **Grupo--**selecione o nome do grupo que contém os nós que deseja atribuir.
   - **Filtro Nome do nó--**permite filtrar os nós disponíveis com base em critérios comuns.

     Observação: o filtro Nome do nó suporta o uso de caracteres curinga.

     Por exemplo, usar o Acc* permite filtrar todos os nós com um nome de nó que comece com Acc. Para limpar os resultados do filtro, clique em X no campo Filtro.
5. Para adicionar nós ao grupo de nós, selecione um ou mais nós que deseja adicionar e clique na seta à direita.

   Os nós passam da lista Nós disponíveis para a lista Nós selecionados e são atribuídos ao grupo de nós.

   Observação: para selecionar e mover todos os nós do grupo atual, clique na seta dupla à direita.
6. (Opcional): para mover todos os nós da lista Nós selecionados para a lista Nós disponíveis, clique na seta simples à esquerda.

   Observação: para selecionar e mover todos os nós do grupo atual, clique na seta dupla à esquerda.
7. Clique em OK.

O Grupo de nós é adicionado.

Modificar grupos de nós

O aplicativo permite modificar os grupos de nós que você criou. Você pode adicionar e remover nós de grupos de nós e alterar o nome de grupos de nós.

Observação: não é possível modificar as seguintes grupos de nós:

- **Todos os nós -** contém todos os nós associados ao aplicativo.
- **Nós sem um grupo** - contém todos os nós associados ao aplicativo que não estão atribuídos a um grupo de nós.
- **Nós sem uma diretiva** - contém todos os nós associados ao aplicativo que não possuem uma diretiva atribuída.
- **SQL Server -** contém todos os nós associados ao aplicativo e o Microsoft SQL Server está instalado.
- **Exchange -** contém todos os nós associados ao aplicativo e o Microsoft Exchange Server está instalado.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na Barra de navegação na página inicial, clique em Nó.

   A tela Nó é exibida.

2. Clique no grupo de nós que deseja modificar e, em seguida, clique em Modificar na barra de ferramentas Grupo de nós.

   A caixa de diálogo Modificar grupo é aberta.

3. Para modificar o Nome do grupo, especifique um novo nome no campo Nome do grupo.

4. Para adicionar nós ao grupo de nós, selecione um ou mais nós para adicionar ao grupo de nós e clique na seta à direita.

   Os nós passam da lista Nós disponíveis para a lista Nós selecionados e são atribuídos ao grupo de nós.

   Observação: para mover todos os nós da lista Nós disponíveis para a lista Nós selecionados, clique na seta dupla à direita.

5. Para remover nós do grupo de nós, clique na seta à esquerda ou na seta dupla à esquerda para remover um dos nós ou todos eles, respectivamente.

6. (Opcional) Para filtrar os nós disponíveis com base em critérios comuns, especifique um valor de filtragem no campo Filtragem pelo nome do nó.

   Observação: o campo Filtro permite o uso de caracteres curinga.

   Por exemplo, usar o Acc* permite filtrar todos os nós com um nome de nó que comece com Acc. Para limpar os resultados do filtro, clique no X no campo Filtro.

7. Clique em OK.

O grupo de nós é modificado.

Observação: ao atribuir um nó do Painel global do CA ARCserve Backup a um grupo de nós, as filiais do CA ARCserve Backup são processadas no nó do Painel global do CA ARCserve Backup, embora nem todas as filiais pertençam ao grupo de nós. Assim, ao selecionar o grupo de nós contento o nó do Painel global do CA ARCserve Backup no aplicativo do CA ARCserve Central Reporting, os relatórios não exibirão dados para todas as filiais do nó do Painel global.

Excluir grupos de nós

É possível excluir um grupo de nós, conforme a necessidade. Quando um grupo que foi adicionado manualmente é excluído, as máquinas virtuais não são removidas do aplicativo. No entanto, se você excluir um grupo que foi criado automaticamente por uma detecção ESX ou vCenter Server, o grupo e todas as máquinas virtuais serão excluídos do aplicativo.

O aplicativo permite excluir os Grupos de nós que você criou.

Não é possível excluir os seguintes grupos de nós:

- **Todos os nós -** contém todos os nós associados ao aplicativo.
- **Nós sem um grupo** - contém todos os nós associados ao aplicativo que não estão atribuídos a um grupo de nós.
- **Nós sem uma diretiva** - contém todos os nós associados ao aplicativo que não possuem uma diretiva atribuída.
- **SQL Server -** contém todos os nós associados ao aplicativo, e o Microsoft SQL Server está instalado nos nós.
- **Exchange -** contém todos os nós associados ao aplicativo, e o Microsoft Exchange Server está instalado nos nós.

Observação: o processo de exclusão dos grupos de nós não exclui nós individuais do aplicativo.

Siga estas etapas:

1. Efetue logon no aplicativo.

   Na barra de navegação na página inicial, clique em Nó para abrir a tela Nó.

2. Clique no grupo de nós que você deseja excluir e, em seguida, clique em Excluir na barra de ferramentas do grupo de nós.

   A caixa de diálogo de Mensagem de confirmação é aberta.

3. Se tiver certeza de que deseja excluir o grupo de nós, clique em Sim.

   Observação: clique em Não se você não deseja excluir o grupo de nós.

O grupo de nós é excluído.

Procurar nós usando a opção Detectar

O Gerenciador do CA ARCserve Central Protection permite procurar nós usando a opção Detectar. O Protection Manager procura nós com base nas informações mantidas no Active Directory de um servidor. O Active Directory fornece as seguintes informações:

- nome do computador
- Informações do sistema operacional (nome, versão, patch)
- Se o Microsoft Exchange Server está no computador
- Se o Microsoft SQL Server está no computador

Para procurar nós usando a opção Detectar

1. Efetue logon no aplicativo.

   Na Barra de navegação na página inicial, clique em Nó.

   A tela Nó é exibida.

2. Na categoria Nó, clique em Detectar para abrir a caixa de diálogo Discover by Active Directory.

3. Preencha os seguintes campos na caixa de diálogo Discover by Active Directory e clique em Adicionar:

   - (Domínio) Nome de usuário
   - (Domínio) Senha
   - Filtragem pelo nome do computador

   Clique em Detectar.

   O processo de detecção (na página 56) é iniciado.

4. Quando a opção Detectar for concluída, a seguinte mensagem de confirmação será exibida:

   `Deseja continuar a adicionar nós a partir do resultado da detecção?`

   Siga um destes procedimentos:

   - Selecione Sim para ir para Adicionar nós a partir do resultado da detecção.
   - Clique em Não para fechar a mensagem.

   Observação: se você selecionar Sim, em seguida, vá para Adicionar nós usando a opção Detectar (na página 55) para obter detalhes.

Tarefas de implantação do CA ARCserve D2D

O Gerenciador do CA ARCserve Central Protection permite implantar remota ou localmente um ou mais nós de modo simultâneo em sistemas de destino. Além disso, é possível adicionar ou editar nós para implantação ou excluir nós da implantação.

Esta seção contém os seguintes tópicos:

Implantar o CA ARCserve D2D para nós

O Gerenciador do CA ARCserve Central Protection permite detectar e implantar a versão mais recente do CA ARCserve D2D para um ou mais nós novos ou existentes.

Observação: para implantar o CA ARCserve D2D em computadores que executam o Windows XP, desative a opção Usar compartilhamento simples de arquivo no computador remoto com Windows XP.

Siga estas etapas:

1. Efetue logon no aplicativo e clique em Nó na barra de navegação.
2. Na tela Nó, clique em Implantar na barra de ferramentas.

   A caixa de diálogo do Contrato de licença será exibida.
3. Leia e aceite os termos do Contrato de Licença e clique em Avançar para abrir a caixa de diálogo Implantação do D2D.
4. Na caixa de diálogo Implantação do D2D, especifique o filtro Nome do nó e do grupo para os nós disponíveis com base em critérios comuns.

   O Nome, Versão e Status de cada nó é exibido.

   Observação: a coluna Versão atual exibe a versão D2D atual do nó está em execução.
5. Clique nas caixas de seleção próximas aos nós ou clique em Selecionar tudo para todos os nós listados sejam implantados ao D2D.

   Observação: ao clicar em Selecionar tudo, a opção muda para Desmarcar todos para a sua conveniência. Além disso, se você selecionar um nó da lista Nós, é possível editar os campos de nó na guia Informações do nó.
6. Clique em Implantar agora para implantar a versão mais recente do D2D exibida na barra de título aos nós.

   Observação: para obter mais informações e o status de implantação em um nó específico, realce o nó e selecione a guia apropriada no painel à direita.

Observação: o Gerenciador do CA ARCserve Central Protection permite instalar, atualizar e implantar a versão mais recente do CA ARCserve D2D para reduzir as versões ou nós sem o CA ARCserve D2D instalado usando o utilitário Implantação do D2D.

Adicionar nós para implantação

O Gerenciador do CA ARCserve Central Protection permite adicionar vários nós para implantação.

Para adicionar nós para implantação

1. Efetue logon no aplicativo e clique em Nó na barra de navegação.
2. Na tela Nó, clique em Implantar na barra de ferramentas.

   A caixa de diálogo do Contrato de licença será exibida.
3. Leia e aceite os termos do Contrato de Licença e clique em Avançar.

   A caixa de diálogo Implantação do D2D é exibida.
4. Clique em Adicionar e preencha os seguintes campos na caixa de diálogo Implantação do D2D:
   - Nome do servidor
   - Nome de usuário
   - Senha
   - Porta
   - Caminho de instalação
   - Permitir que o programa de instalação instale o driver (selecionado por padrão)
   - Reinicialização (o padrão é Sim)

     Se o nó for implantado com uma reinicialização bem-sucedida (Sim), ele será adicionado à lista de nós gerenciada pelo CA ARCserve Central Applications.

     Se o nó for implantada sem a opção de reinicialização (Não), ele será adicionado ao grupo de nós não gerenciados pelo CA ARCserve Central Applications.
   - Use o HTTPS (o padrão é Nenhum)

     A comunicação HTTPS (segura) fornece um nível maior de segurança do que a comunicação HTTP. O HTTPS é o protocolo de comunicação recomendado se você transmite informações confidenciais pela rede.

   Observação: é possível ver os nós adicionados no filtro Todos os nós e Não agrupado.
5. Clique em OK para adicionar os nós.

Editar nós para implantação

O Gerenciador do CA ARCserve Central Protection permite editar nós para implantação.

Para editar nós para implantação

1. Efetue logon no aplicativo e clique em Nó na barra de navegação.
2. Na tela Nó, clique em Implantar na barra de ferramentas.

   A caixa de diálogo do Contrato de licença será exibida.
3. Leia e aceite os termos do Contrato de Licença e clique em Avançar.

   A tela Implantação do D2D é exibida.
4. Selecione o nó que deseja editar para implantação e clique em Editar para abrir a caixa de diálogo Editar.
5. Na caixa de diálogo Editar, edite os dados que deseja alterar e clique em OK.

Excluir nós da implantação

O Gerenciador do CA ARCserve Central Protection permite excluir um ou mais nós da implantação.

Para excluir nós da implantação

1. Efetue logon no aplicativo e clique em Nó na barra de navegação.
2. Na tela Nó, clique em Implantar na barra de ferramentas.

   A caixa de diálogo do Contrato de licença será exibida.
3. Leia e aceite os termos do Contrato de Licença e clique em Avançar.

   A tela Implantação do D2D é exibida.
4. Selecione um ou mais nós a serem excluídos da implantação.
5. Clique em Excluir para excluir os nós da implantação do D2D.

Filtrar grupos de nós

O Gerenciador do CA ARCserve Central Protection permite usar filtros para exibir nós de um grupo com determinado aplicativo instalado. O Gerenciador do CA ARCserve Central Protection permite filtrar os seguintes aplicativos:

- CA ARCserve Backup
- CA ARCserve D2D
- Microsoft SQL Server
- Microsoft Exchange Server

Para filtrar grupos de nós

1. Efetue logon no Gerenciador do CA ARCserve Central Protection.

   Na Barra de navegação na página inicial, clique em Nó.

   A tela Nó é exibida.

2. Na lista de grupos, clique no grupo que deseja filtrar.

   Observação: é possível filtrar todos os grupos padrão (Todos os nós, Não atribuído, SQL Server, Exchange) e todos os grupos com nomes personalizados.

   Na barra de ferramentas Filtro, clique na caixa de seleção ao lado do aplicativo que deseja filtrar.

O grupo de nós é filtrado.

Como gerenciar diretivas do CA ARCserve D2D

O Gerenciador do CA ARCserve Central Protection fornece várias ferramentas e opções que podem ser usadas para gerenciar diretivas do CA ARCserve D2D. Esta seção contém informações sobre como adicionar, excluir, modificar, implantar o D2D e copiar diretivas em servidores remotos. É possível criar diretivas centralizadas de backup que podem ser distribuídas simultaneamente para vários nós gerenciados.

A seguir são relacionados alguns exemplos comuns para diretivas centralizadas de backup:

- Programações
- Tarefas
- Destinos
- Eventos
- Configurações

Esta seção contém os seguintes tópicos:

Criar diretivas

O Gerenciador do CA ARCserve Central Protection permite criar uma ou mais diretivas para atribuir a nós do D2D.

Siga estas etapas:

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação para abrir a tela Diretivas.
2. Clique em Novo para abrir a caixa de diálogo Nova diretiva.
3. Digite o nome de diretiva e preencha os campos necessários nas guias Configurações de backup (na página 82), Definições da cópia de arquivo (na página 99), Copiar pontos de recuperação (na página 115) e Preferências (na página 119).
4. Clique em Salvar.

A nova diretiva é salva e exibe uma mensagem perguntando se deseja atribuí-la aos nós agora. Ao clicar em Não, a nova diretiva é exibida na tela Diretivas. Ao clicar em Sim, a tela Executar/cancelar atribuição de diretiva (na página 133) é exibida.

Gerenciar configurações de backup

As configurações de backup permitem definir comportamentos como a origem e o destino do backup, a programação de cada tipo de backup, bem como as configurações usuais e avançadas para as tarefas de backup. Estas configurações podem ser modificadas a qualquer momento na tela Diretivas.

Para gerenciar as configurações de backup, clique em Diretivas na barra de navegação na página inicial e clique em Novo.

Esta seção contém os seguintes tópicos:

Especificar configurações de proteção

O Gerenciador do CA ARCserve Central Protection permite especificar as configurações de proteção para os dados que desejar armazenar em backup.

Para especificar configurações de proteção

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação.

   A tela Diretivas é exibida.

2. Clique em Novo para criar uma diretiva.

   A caixa de diálogo Nova diretiva é aberta, exibindo a opção Configurações de proteção da guia Configurações de backup.

3. Especificar o **destino do backup**.

   É possível especificar um caminho local (volume ou pasta) ou uma pasta compartilhada remota (ou unidade mapeada) para o local do backup.

   a. Se você especificar a execução do backup em seu caminho local (volume ou pasta), o destino de backup especificado não pode ser o mesmo local da origem do backup. Se a origem for incluída no destino por engano, a tarefa de backup ignorará essa parte da origem e não a incluirá no backup.

Por exemplo, se estiver tentando fazer backup do computador local inteiro, que consiste nos volumes C, D e E, e também especificar o volume E como destino, o CA ARCserve D2D só fará backup dos volumes C e D no volume E. Os dados do volume E não serão incluídos no backup. Para fazer backup de todos os volumes locais, especifique um local remoto para o destino.

Importante: Verifique se o volume de destino especificado não contém informações do sistema, caso contrário, ele não será protegido (armazenado em backup), e o sistema não se recuperará após a BMR (Bare Metal Recovery - Recuperação Bare Metal), se ela for necessária.

Observação: discos dinâmicos não podem ser restaurados no nível do disco. Se o backup dos dados for feito no volume de um disco dinâmico, você não poderá restaurar este disco durante a BMR.

b. Se você optar por fazer backup em um local compartilhado remoto, é obrigatório especificar um caminho local ou procurar o local e fornecer credenciais de usuário (nome de usuário e senha) para acessar o computador remoto.

c. Se o destino de backup especificado tiver sido alterado desde a execução do último backup, será preciso selecionar o tipo de backup. Essas opções serão ativadas quando você alterar o destino do backup. As opções disponíveis são Backup completo e Backup incremental.

- **Backup completo--** especifica que o próximo backup executado será um backup completo. O novo destino de backup não tem nenhuma dependência no destino de backup antigo. Se você continuar com um backup completo, o local anterior não será mais necessário para que os backups continuem. Pode-se optar por manter o backup antigo para qualquer restauração ou excluí-lo, caso não queira executar nenhuma restauração a partir desse local. Isto não afetará backups futuros.

- **Backup incremental--**especifica que o próximo backup executado será um backup incremental. O próximo backup incremental para o novo destino será executado sem copiar todos os backups do destino anterior. No entanto, o novo local depende do local anterior, pois as alterações incluirão somente os dados incrementais (não os dados do backup completo). Não exclua os dados do local anterior. Suponhamos que você altere o destino do backup para outra pasta e tente executar um backup incremental. Se o primeiro destino de backup não existir, haverá falha no backup.

4. Especificar a **origem do backup**.

   Você pode especificar o backup do computador inteiro ou um volume individual no seu computador.

   - **Fazer backup da máquina inteira**--especifica o backup de toda a máquina. Todos os volumes da máquina serão armazenados em backup.

     Observação: se a opção de backup completo do computador for selecionada, o CA ARCserve D2D detectará automaticamente todos os discos e volumes acoplados ao computador atual e os incluirá no backup.

     Por exemplo, se um novo disco estiver acoplado ao computador depois que as definições de backup tiverem sido configuradas, não será preciso alterar as configurações de backup, e os dados no novo disco serão protegidos automaticamente.

   - **Selecionar os volumes individuais para fazer backup**--esse recurso de filtragem de volume permite especificar o backup apenas dos volumes selecionados. No entanto, se você especificar um volume que não existe no servidor remoto do CA ARCserve D2D, o volume é ignorado automaticamente durante o backup. Por exemplo, especifique fazer backup de volumes C, D e E; e atribua-os ao servidor do CA ARCserve D2D que contém apenas os volumes C e D. A diretiva é atribuída aos volumes C e D para o servidor do CA ARCserve D2D e o volume E é ignorado com uma mensagem de aviso salva no log de atividades.

     Você tem também a opção para selecionar ou cancelar a seleção de todos os volumes listados.

     Observação: se alguns volumes forem explicitamente selecionados para backup, apenas os volumes selecionados serão armazenados em backup.

     Uma mensagem de notificação será exibida se ocorrer a seguinte condição:

     - **Relacionado a BMR--**se o volume de sistema/inicialização não estiver selecionado para backup, uma mensagem de aviso será exibida para notificá-lo de que o backup não pode ser usado para BMR.

5. Especifique a **Configuração de retenção**.

   Você pode definir a diretiva de retenção com base no número de pontos de recuperação a serem retidos (mescla sessões) ou com base no número de conjuntos de recuperação a serem retidos (exclui conjuntos de recuperação e desativa os itens incrementais ininterruptos).

   - Ponto de recuperação – Esta é a opção recomendada. Com esta opção selecionada, é possível aproveitar totalmente os recursos de backup incremental ininterrupto e economizar espaço de armazenamento.
   - Conjunto de recuperação – Esta opção geralmente é usada para ambientes de armazenamento de grande porte. Com esta opção selecionada, é possível criar e gerenciar conjuntos de backup que o ajudam a gerenciar o tempo da janela de backup de forma mais eficiente quando você está protegendo uma grande quantidade de dados. É possível usar esta opção quando o tempo de backup for uma prioridade em relação às restrições de espaço.

   Padrão: Reter pontos de recuperação

   Reter pontos de recuperação

   Selecione essa opção para especificar o número de pontos de recuperação (imagens completas, incrementais e de backup de verificação) a serem retidos.

   - **Especifique o número de pontos de recuperação a ser retido**

     Quando o limite especificado é excedido, o CA ARCserve D2D mescla o primeiro backup incremental filho (o mais antigo) com o backup pai para criar uma nova imagem de linha de base que inclui o bloco pai e o bloco filho mais antigo. O ciclo de mesclagem do backup filho mais antigo com o backup pai se repetirá para cada backup subsequente, permitindo executar backups incrementais ininterruptamente, enquanto mantém a mesma contagem de retenção.

     Observação: se o destino não tiver espaço livre suficiente, considere reduzir a quantidade de pontos de recuperação salva.

     Padrão: 31

     Mínimo: 1

Máximo: 1344

- **Executar a tarefa de mesclagem** -- selecione uma das seguintes opções ao executar a tarefa de mesclagem:
  - **O quanto antes** -- selecione esta opção para executar a tarefa de mesclagem a qualquer momento.
  - **Cada dia durante o intervalo abaixo** -- selecione essa opção para executar a tarefa de mesclagem em um intervalo específico. Definir um intervalo de tempo ajuda a evitar que a tarefa de mesclagem introduza operações de E/S em excesso no servidor de produção ao executar a tarefa de mesclagem por um longo período.

    Observação: ao definir o intervalo de tempo para execução da tarefa de mesclagem, certifique-se de especificar um intervalo de tempo que permitirá que as tarefas de backup relacionadas sejam concluídas antes do início da mesclagem.

Reter conjuntos de recuperação

Selecione essa opção para especificar o número de conjuntos de recuperação a serem retidos. Com essa configuração, você pode desativar os backups incrementais ininterruptos definitivamente, sem mesclar nenhuma sessão. O uso de conjuntos de recuperação ajuda a resolver a questão do tempo levado para concluir tarefas de mesclagem.

- **Especifique o número de conjuntos de recuperação a ser retido**

  Selecione essa opção para especificar o número de conjuntos de recuperação retidos. Um conjunto de recuperação é uma série de backups, iniciando com um backup completo e, em seguida, backups incrementais, de verificação ou completos.

  Conjunto de exemplo 1:

  - Completo
  - Incremental
  - Incremental
  - Verificar
  - Incremental

Conjunto de exemplo 2:

- Completo
- Incremental
- Completo
- Incremental

Um backup completo é necessário para iniciar um novo conjunto de recuperação. O backup que inicia o conjunto é convertido automaticamente em um backup completo, mesmo se nenhum backup completo está configurado ou programado para ser executado no momento.

Observação: um conjunto de recuperação incompleto não é contado ao calcular um conjunto de recuperação existente. Um conjunto de recuperação é considerado concluído somente quando o backup inicial do próximo conjunto de recuperação é criado.

Padrão: 2

Mínimo: 1

Máximo: 100

Observação: quando desejar excluir um conjunto de recuperação para poupar o espaço de armazenamento de backup, reduza o número de conjuntos retidos, e o CA ARCserve D2D excluirá automaticamente o conjunto de recuperação mais antigo. Não tente excluir o conjunto de recuperação manualmente.

Exemplo 1 - conjunto de recuperação:

- A hora de início do backup é às 6h00 de 20 de agosto de 2012.
- Um backup incremental é executado a cada 12 horas.
- Um novo conjunto de recuperação começa no último backup na sexta-feira.
- Você deseja reter três conjuntos de recuperação.

Neste exemplo, um backup incremental é executado diariamente às 06:00 e às 18:00. O primeiro conjunto de recuperação é criado quando o primeiro backup (deve ser um backup completo) é realizado. Em seguida, o primeiro backup completo é marcado como o backup inicial do conjunto de recuperação. Quando o backup programado para as 18:00 na sexta-feira for executado, ele será convertido em backup completo, e o backup será marcado como o backup inicial do conjunto de recuperação.

Exemplo 2 - conjunto de recuperação:

- Especifique o número de conjuntos de recuperação a serem retidos como 1.

Observação: o CA ARCserve D2D sempre mantém dois conjuntos de modo que um conjunto completo é mantido antes de iniciar o próximo conjunto de recuperação.

Exemplo 3 - conjunto de recuperação:

- Especifique o número de conjuntos de recuperação a serem retidos como 2.

Observação: o CA ARCserve D2D excluirá o primeiro conjunto de recuperação quando o quarto estiver pronto para iniciar a recuperação. A execução desta ação garante que, quando o primeiro backup for excluído, e o quarto estiver sendo iniciado, você ainda terá dois conjuntos de recuperação (conjunto de recuperação 2 e conjunto de recuperação 3) disponíveis no disco.

Mesmo se apenas um conjunto de recuperação for mantido, será necessário espaço para ao menos dois backups completos.

– **Iniciar um novo conjunto de recuperação a cada:**

  - **Dia da semana selecionado** -- especifica o dia da semana selecionado para iniciar um novo conjunto de recuperação.
  - **Dia do mês selecionado** -- especifica o dia do mês selecionado para iniciar um novo conjunto de recuperação. Escolha um dia entre 1 e 30 ou, se o mês tiver 28, 29, 30 ou 31 dias, especifique o último dia do mês para criar o conjunto de recuperação.

- **Iniciar um novo conjunto de recuperação com:**
  - **Primeiro backup no dia selecionado** -- especifica o dia da semana selecionado para iniciar um novo conjunto de recuperação.
  - **Último backup no dia selecionado** -- indica que você deseja iniciar um novo conjunto de recuperação com o último backup programado no dia especificado. Se o último backup for selecionado para iniciar o conjunto e, por qualquer motivo, ele não for executado, o próximo backup programado iniciará o conjunto convertendo-o em um backup completo. Se o próximo backup for executado ad hoc (por exemplo, uma situação de emergência requer um backup incremental rápido), você poderá decidir se deseja executar um backup completo para iniciar o conjunto de recuperação ou executar um backup incremental para que o próximo backup inicie o conjunto de recuperação.

    Observação: o último backup pode não ser o último backup do dia quando você executa um backup ad hoc.

6. Especificar o tipo de **compactação**.

   Selecione esta opção para especificar o tipo de compactação que deseja usar para os backups.

   A compactação reduz o uso de espaço em disco, mas também tem um impacto inverso sobre a velocidade do backup, devido ao aumento no uso da CPU.

   As opções de compactação disponíveis são as seguintes:

   - **Nenhuma compactação**

     Nenhuma compactação será executada. Essa opção exige menos uso da CPU (mais velocidade), mas também mais uso de espaço em disco para a imagem de backup.

   - **Compactação padrão**

     Alguma compactação será realizada. Essa opção proporciona um bom equilíbrio entre o uso da CPU e o uso do espaço em disco. Essa é a configuração padrão.

   - **Compactação máxima**

     A compactação máxima será realizada. Essa opção proporciona maior uso da CPU (menos velocidade), mas também menos uso de espaço em disco para a imagem de backup.

Esteja ciente dos seguintes cenários:

- Se a imagem de backup contiver dados não compactáveis (como imagens JPG, arquivos ZIP etc.), pode ser necessário espaço adicional de armazenamento alocado para lidar com esses dados. Caso especifique opções de compactação e a origem de backup contiver dados que não podem ser compactados, você perceberá um aumento geral no uso de espaço em disco.
- Se alterar o nível de compactação de nenhuma compactação para compactação padrão ou compactação máxima; ou ainda se você alterar o nível de compactação de compactação padrão ou compactação máxima para nenhuma compactação, o primeiro backup executado após a alteração no nível de compactação será um backup completo. Após a execução do backup completo, todos os backups futuros (completo, incremental ou de verificação) serão executados conforme a programação.
- Se o destino não tiver espaço livre suficiente, considere aumentar a configuração de compactação do backup.

7. Especificar as configurações de **criptografia**.

   a. Selecione o tipo de algoritmo de criptografia que deseja usar para os backups.

      A criptografia de dados é a conversão de dados em uma forma ininteligível sem um mecanismo decodificador. A proteção de dados do CA ARCserve D2D usa algoritmos de criptografia seguros AES (padrão de criptografia avançada) para atingir o máximo de segurança e privacidade dos dados especificados.

      As opções de formatação são Sem criptografia, AES-128, AES-192 e AES-256. (Para desativar criptografia, selecione Sem criptografia.)

      - Um backup completo e todos os seus respectivos backups incrementais e de verificação deverão usar o mesmo algoritmo de criptografia.
      - Se o algoritmo de criptografia para um backup incremental ou de verificação for alterado, um backup completo deverá ser executado. Isso significa que, após a alteração de algoritmo de criptografia, o primeiro backup será completo, independentemente do tipo de backup original.

        Por exemplo, se você alterar o formato do algoritmo e enviar um backup personalizado incremental ou de verificação manualmente, ele é convertido automaticamente para um backup completo.

b. Quando um algoritmo de criptografia é selecionado, você deve fornecer (e confirmar) uma senha de criptografia.

   - A senha de criptografia é limitada a um máximo de 23 caracteres.
   - Um backup completo e todos os seus respectivos backups incrementais e de verificação deverão usar a mesma senha para criptografar dados.
   - Se a senha de criptografia para um backup incremental ou de verificação for alterada, um backup completo deverá ser executado. Isso significa que, após a alteração de senha de criptografia, o primeiro backup será completo, independentemente do tipo de backup.

     Por exemplo, se você alterar a senha de criptografia e enviar um backup personalizado incremental ou de verificação manualmente, ele será convertido automaticamente para um backup completo.

c. O CA ARCserve D2D fornece gerenciamento de senha de criptografia para que você não precise se lembrar de senhas de criptografia.

   - A senha também será criptografada.
   - A senha será lembrada e não será necessária se você restaurar para a mesma máquina.
   - A senha é necessária se você restaurar em um computador diferente.
   - A senha não é obrigatória se você estiver tentando exportar um ponto de recuperação que contenha dados criptografados e o ponto de recuperação pertencer a backups executados na máquina atual.
   - A senha é sempre obrigatória se você estiver tentando recuperar dados criptografados de um ponto de recuperação exportado.
   - A senha não é necessária para navegar para um ponto de recuperação criptografado.
   - A senha é necessária para executar uma BMR.

d. Quando a criptografia estiver ativada, o log de atividades será atualizado.

   - Uma mensagem será gravada no log de atividades para descrever o algoritmo de criptografia selecionado para cada backup.
   - Uma mensagem será gravada no log de atividades para indicar que um backup incremental ou de verificação foi convertido para um backup completo (alteração de senha ou alteração do algoritmo).

Observação: configurações de criptografia não precisam permanecer as mesmas para seus backups. Você pode alterar essas configurações a qualquer momento, inclusive após alguns backups dos mesmos dados.

8. Especifique o **Acelerador de backup**.

   Você pode especificar a velocidade máxima (MB/min) em que os backups serão gravados. Você pode restringir a velocidade de backup para reduzir a utilização da CPU ou da rede. No entanto, ao limitar a velocidade de backup, isso terá um efeito negativo na janela de backup. Ao reduzir a velocidade máxima do backup, você aumentará a quantidade de tempo para a execução do backup.

   Observação: por padrão, a opção Aceleração de backup não está ativada e a velocidade de backup não é controlada.

9. Clique em Salvar.

As configurações de proteção são salvas.

Especificar programações de backup

O Gerenciador do CA ARCserve Central Protection permite especificar programações de backups.

Para especificar programações de backup

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação.

   A tela Diretivas é exibida.

2. Clique em Novo para criar uma diretiva.

   A caixa de diálogo Nova diretiva é aberta.

3. Clique na guia Programar.

   A caixa de diálogo de opções Programar é exibida.

4. Especificar as opções de programação de backup.

   - **Definir data e hora de início**--especifica a data e a hora de início para seus backups programados.

     Observação: Ao definir o intervalo entre as tarefas de backup de repetição, certifique-se de deixar tempo suficiente para permitir que a tarefa anterior e eventuais tarefas de mesclagem relacionadas sejam concluídas antes que a próxima tarefa de backup seja iniciada. O valor de tempo pode ser estimado com base no seu próprio ambiente e histórico de backup específicos.

   - **Backup incremental--**especifica a programação de backups incrementais.

     Conforme programado, o CA ARCserve D2D faz backup incremental apenas dos blocos que foram alterados desde o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a execução de backups e você deve usá-la por padrão.

     As opções disponíveis são Repetir e Nunca. Se você selecionar a opção Repetir, então, é preciso especificar também o tempo decorrido (em minutos, horas, dias) entre as tentativas de backup. A configuração mínima para os backups incrementais é a cada 15 minutos.

     Por padrão, os backups incrementais são programados para serem repetidos uma vez por dia.

   - **Backup completo--**especifica a programação de backups completos.

     Conforme programado, o CA ARCserve D2D executará um backup completo de todos os blocos do computador de origem. As opções disponíveis são Repetir e Nunca. Se você selecionar a opção Repetir, então, é preciso especificar também o tempo decorrido (em minutos, horas, dias) entre as tentativas de backup. A configuração mínima para os backups completos é a cada 15 minutos.

     Por padrão, a programação para backups completos é Nunca (nenhuma repetição programada).

   - **Backup de verificação--**especifica a programação de backups de verificação.

     Conforme o programado, o CA ARCserve D2D verificará se os dados protegidos estão válidos e íntegros executando uma verificação de confiabilidade para a imagem de backup armazenada na origem do backup e sincronizará novamente essa imagem, se necessário. Um backup de verificação examinará o backup mais recente de cada bloco e irá comparar o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup de qualquer bloco não corresponder à origem (possivelmente devido a alterações no sistema desde o último backup), o CA ARCserve D2D atualizará (fará nova sincronização) o backup do bloco que não corresponder. Um backup de verificação também pode ser usado (muito raramente) para proporcionar a mesma garantia que a do backup completo, mas sem usar a mesma quantidade de espaço.

A vantagem de um backup de verificação é que ele produz uma imagem de backup muito pequena quando comparado ao backup completo porque somente os blocos alterados (que não coincidirem com o último backup) são armazenados em backup. A desvantagem de um backup de verificação é a lentidão, pois o CA ARCserve D2D precisa comparar todos os blocos do disco de origem com os blocos do último backup.

As opções disponíveis são Repetir e Nunca. Se você selecionar a opção Repetir, então, é preciso especificar também o tempo decorrido (em minutos, horas, dias) entre as tentativas de backup. A configuração mínima para os backups de verificação é a cada 15 minutos.

Por padrão, a programação para backups de verificação é Nunca (nenhuma repetição programada).

5. Clique em Salvar.

As configurações de programação de backup são salvas.

Observação: se em um determinado momento houver mais de um tipo de backup programado para execução simultânea, o tipo de backup que será executado terá como base as seguintes prioridades:

- Prioridade 1 - Backup completo
- Prioridade 2 - Backup de verificação
- Prioridade 3 - Backup incremental

Por exemplo, se você tem todos os três tipos de backup programados para execução ao mesmo tempo, o CA ARCserve D2D irá executar o backup completo. Se não houver nenhum backup completo programado, mas um backup de verificação e um incremental para execução ao mesmo tempo, o CA ARCserve D2D executará o backup de verificação. Um backup incremental programado só será executado se não houver conflito com nenhum outro tipo de backup.

Especificar configurações avançadas de backup

O Gerenciador do CA ARCserve Central Protection permite especificar configurações avançadas para os backups.

Para especificar configurações de backup avançadas

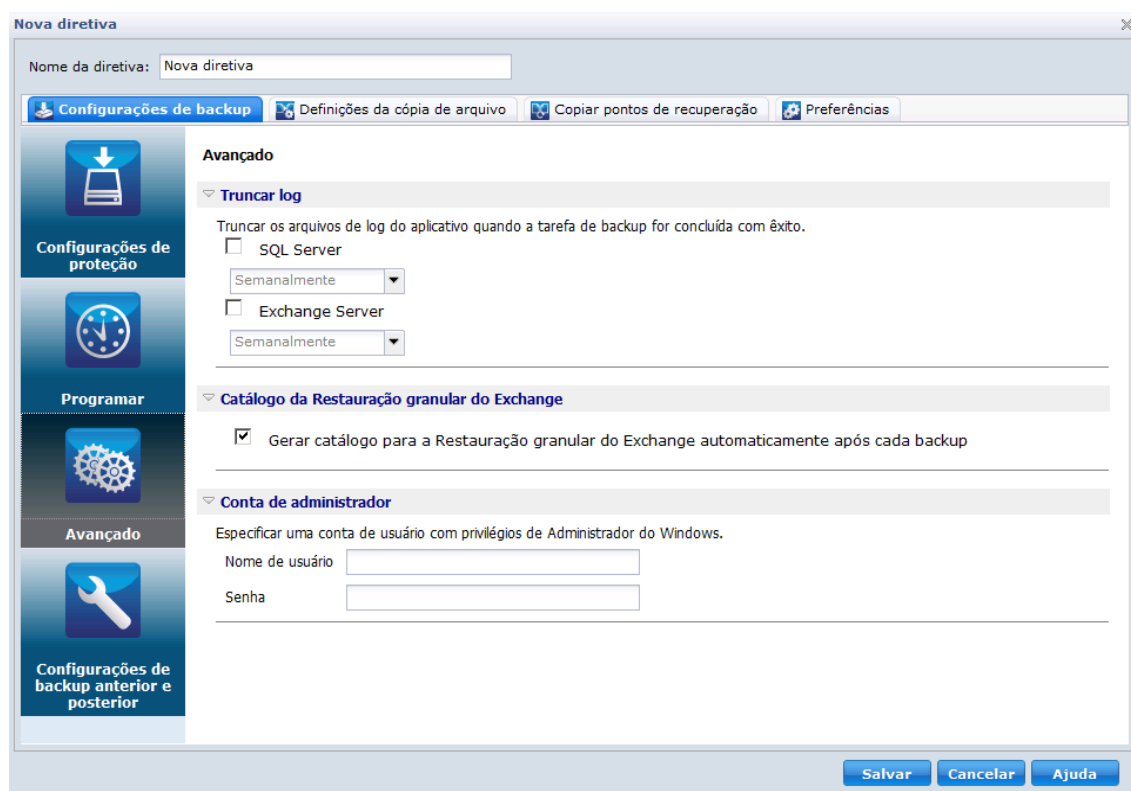
1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação.

   A tela Diretivas é exibida.

2. Clique em Novo para criar uma diretiva.

   A caixa de diálogo Nova diretiva é aberta.

3. Clique na guia Avançado.

   A caixa de diálogo Configurações avançadas é exibida.

4. Especifique as opções de configuração de ações avançadas.

   - **Truncar log**--especifica o truncamento de arquivos de log de transações acumulados para os aplicativos selecionados após o próximo backup realizado com êxito.

     Os backups do CA ARCserve D2D consistem em uma imagem de instantâneo e em arquivos de log de transações que foram criados para ele. Em determinado momento, os arquivos de log de transações (confirmadas) mais antigos não são mais necessários e devem ser eliminados para liberar espaço para novos arquivos de log. O processo de limpeza desses arquivos de log é chamado de truncamento de log. Esta opção permite o truncamento de arquivos de log de transações confirmados, o que poupará o espaço em disco.

     As opções disponíveis são SQL Server e Exchange Server. Você pode selecionar ambos ou nenhum desses aplicativos. Se selecionar um dos aplicativos, também é possível especificar um período (diariamente, semanalmente, mensalmente) programado para truncamento automático de log:

     Observação: os arquivos de log de transações não podem ser truncados sem a execução de um backup bem-sucedido.

     - **Diariamente -** no dia seguinte ao da conclusão bem-sucedida do backup, os logs de transação confirmados serão limpos imediatamente.
     - **Semanalmente -** depois de sete dias, os logs de transações confirmadas serão eliminados imediatamente após a conclusão bem-sucedida do backup.
     - **Mensalmente -** depois de 30 dias, os logs de transação confirmados serão removidos imediatamente após a conclusão bem-sucedida do backup.

     Se uma tarefa de backup já estiver em execução ao mesmo tempo em que a limpeza estiver programada para ser executada, a operação de limpeza será movida para a próxima tarefa programada.

     Por exemplo:

     Você programou um backup incremental para ser executado automaticamente todo dia às 17:00, mas iniciou um backup completo manualmente às 16:55. Suponhamos que o backup seja concluído com êxito às 17:10.

     Nesse caso, o backup incremental que foi programado para 17:00 não será executado, pois o backup completo ad hoc ainda estará em andamento. Então, os arquivos de log de transações confirmados serão limpos após a próxima tarefa de backup bem-sucedida. Nesse caso, ele será executado um dia após a conclusão bem-sucedida do backup incremental programado às 17:00.

- **Restauração granular do Exchange--**especifica se é preciso ou não ativar os backups de restauração granular do Exchange (que gera os catálogos de restauração granular do Exchange durante cada backup).

  Um backup de Restauração granular do Exchange captura informações sobre a mensagem de email, a pasta de email e os níveis de caixa de correio do Exchange em um um backup de passagem única pelo banco de dados do Exchange. Com esta opção ativada, é possível executar recuperações granular do banco de dados do Exchange selecionando uma lista de objetos no Exchange, bem como especificar exatamente o que deseja recuperar sem precisar recuperar ou despejar o banco de dados do Exchange em um local diferente.

  - A vantagem de ativar essa opção é que, com um catálogo de Restauração granular do Exchange, não é preciso esperar muito tempo para executar uma busca de restauração.
  - A desvantagem de ativar essa opção é que gerar um catálogo de restauração granular durante cada backup resulta em um aumento na janela de backup e na carga de trabalho. O CA ARCserve D2D deve acessar cada caixa de correio, autenticar e compilar as informações granulares, o que, considerando o número de caixas de correio e o tamanho dos dados, pode ser demorado.
  - Se você desativar a Restauração granular do Exchange, o CA ARCserve D2D salvará apenas as informações básicas do Exchange. Antes de restaurar, você tem a oportunidade de gerar um catálogo de restauração granular do Exchange nesse momento.

- **Conta de administrador--**especifica um nome de usuário e uma senha com direitos de acesso para executar o backup. O CA ARCserve D2D verifica se o nome e a senha são válidos e se o usuário pertence a um grupo de administradores.

  Esteja ciente do seguinte:

  - Para especificar uma conta de domínio, o formato de nome de usuário deve corresponder a um nome de usuário de domínio totalmente qualificado no formato "<nome_de_dominio>\<nome_de_usuario>".
  - Se as informações da conta de administrador para o servidor do CA ARCserve D2D forem alteradas (nome de usuário/senha), recomendamos reconfigurar as informações da conta de administrador nessa caixa de diálogo.
  - Se não forem especificadas as credenciais de conta de administrador, o CA ARCserve D2D irá inserir automaticamente as informações da conta em que a diretiva será implantada.

5. Clique em Salvar.

As configurações avançadas de backup são salvas.

Especificar as configurações de backup anterior e posterior

O Gerenciador do CA ARCserve Central Protection permite especificar as definições de backup.

Para especificar configurações de backup anterior/posterior

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação.

   A tela Diretivas é exibida.

2. Clique em Novo para criar uma diretiva.

   A caixa de diálogo Nova diretiva é aberta.

3. Clique na guia Configurações de backup anterior e posterior.

   A caixa de diálogo Configurações de backup anterior e posterior é exibida.

4. Especificar as opções de configuração de backup.

   - **Ações--**especifica a execução de comandos de script para ações que devem ser executadas antes do início do backup, depois de a imagem do instantâneo ser capturada e/ou após a conclusão do backup. Você também pode acionar o comando de script com base em códigos de saída específicos e selecionar a ação a ser executada (executar ou cancelar a tarefa) quando esse código de saída for retornado.
     - A ação Executar tarefa orienta o CA ARCserve D2D a continuar a executar a tarefa, se o código de saída especificado for retornado.
     - A ação Cancelar tarefa orienta o CA ARCserve D2D a cancelar a tarefa, se o código de saída especificado for retornado.

5. Clique em Salvar.

As configurações de backup anterior e posterior são salvas.

Gerenciar configurações da cópia de arquivo

Antes de executar a primeira tarefa de cópia de arquivo, é necessário especificar as configurações e diretivas da cópia de arquivo. Essas configurações permitem especificar comportamentos, como a origem dos dados da cópia de arquivo, o destino para os arquivos copiados, a programação para cada tarefa de cópia de arquivo e as configurações e filtros aplicados às tarefas de cópia de arquivo. Estas configurações podem ser modificadas a qualquer momento na tela Diretivas.

Especificar origens de cópias de arquivos

O Gerenciador do CA ARCserve Central Protection permite especificar os arquivos de origem para cópia de arquivo para um destino específico.

Para especificar origens de cópias de arquivos

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação.

   A tela Diretivas é exibida.

2. Clique em Novo para criar uma diretiva.

   A caixa de diálogo Nova diretiva é aberta.

3. Selecione a guia Definições da cópia de arquivo.

   A caixa de diálogo Origem das definições da cópia de arquivo é exibida.

4. Selecione a opção Ativar cópia de arquivo para validar e salvar as alterações nas configurações de cópia de arquivo. Esta opção é ativada, por padrão.

5. Especifique as configurações da origem da cópia de arquivo.

   Origens da cópia de arquivo

   Permite especificar manualmente as origens da cópia de arquivo, juntamente com a diretiva correspondente (filtros) e o tipo de cópia de arquivo (copiar e manter ou copiar e mover) a ser executado após cada backup do CA ARCserve D2D realizado com êxito. Estas origens de cópia de arquivo podem ser adicionadas, removidas ou modificadas.

   Observação: o CA ARCserve D2D não copiará arquivos de aplicativos, arquivos com atributos do sistema e arquivos com atributos temporário.

   - **Add Source**

     Quando você clica nessa opção, a caixa de diálogo Tipo de diretiva é aberta, para a seleção do tipo de tarefa de cópia de arquivo a ser executada (copiar e manter ou copiar e mover). Após selecionar o tipo de diretiva, a caixa de diálogo Diretiva da cópia de arquivo correspondente é aberta para que possa adicionar uma origem a ser copiada e especificar as diretivas correspondentes para essa origem. Para obter mais informações, consulte o tópico Especificar diretivas de cópia de arquivo (na página 101).

Observação: apenas uma origem atual cujo backup foi feito está qualificada para a cópia de arquivo. Não é possível adicionar uma origem de um volume que não tenha sido previamente submetido a backup pelo CA ARCserve D2D.

- **Remover**

  Ao clicar nesta opção, a origem selecionada será removida da lista exibida.

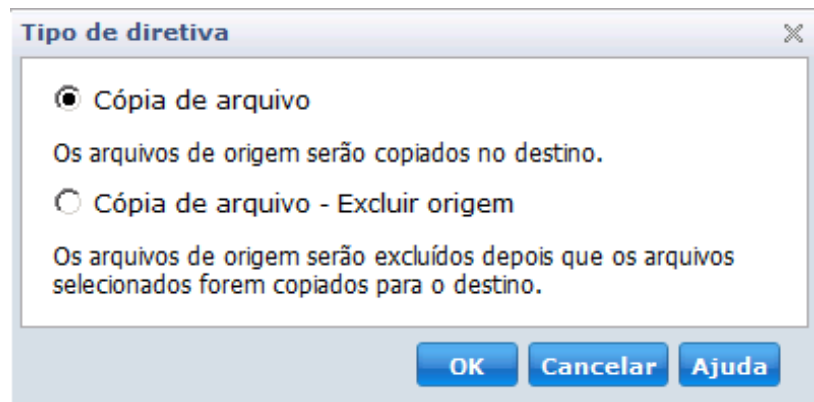
- **Modificar**

  Clicar nesta opção abre a caixa de diálogo Diretivas da cópia de arquivo para que seja possível alterar as configurações de diretiva para a origem selecionada. Para obter mais informações, consulte o tópico Especificar diretivas de cópia de arquivo (na página 101).

6. Clique em Salvar configurações.

As configurações da cópia de arquivo são salvas.

Especifique as diretivas da cópia de arquivo

Quando você clica na opção Adicionar origem para cópia de arquivo, a caixa de diálogo Tipo de diretiva é aberta para a seleção inicial do tipo de tarefa de cópia de arquivo a ser executada.

Os tipos disponíveis são Cópia de arquivo e Cópia de arquivo - excluir origem.

Cópia de arquivo

Os dados são copiados da origem ao de destino (permanece no local de origem) e fornece várias versões armazenadas.

Cópia de arquivo - excluir origem

Os dados são movidos da origem ao destino (excluídos do local de origem), fornecendo mais espaço livre disponível em sua origem.

Quando você seleciona a opção Cópia de arquivo - excluir origem, uma mensagem de aviso é exibida imediatamente, alertando que os dados de cópia de arquivo do arquivo especificado serão excluídos e não estarão mais disponíveis no local de origem original. É necessário clicar em OK para ir para a caixa de diálogo Diretivas de cópia de arquivo.

Importante! Para arquivos copiados usando a opção Cópia de arquivo - excluir origem o CA ARCserve D2D deixará um arquivo de fragmento com a extensão "D2DARC". O arquivo de fragmento contém informações sobre o destino e sobre quando os arquivos foram movidos.

Quando você especifica o tipo de diretiva para excluir a origem dos dados armazenados em backup, há diretivas relacionadas que também precisam ser especificadas. Na caixa de diálogo Configurações de cópia de arquivo, se desejar adicionar uma nova origem de cópia de arquivo ou modificar uma origem de cópia de arquivo existente, a caixa de diálogo Diretivas de cópia de arquivo permitirá que as diretivas sejam especificadas.

Dependendo do tipo de diretiva selecionada, uma caixa de diálogo Diretivas de cópia de arquivo diferente será exibida; no entanto, as seleções são semelhantes.

Cópia de arquivo selecionada:

Cópia de arquivo - excluir origem selecionada:

Cópia de arquivo - excluir origem

Permite especificar a origem da cópia de arquivo e o conjunto de diretivas correspondentes, bem como o tipo de cópia de arquivo a ser executado. É possível procurar o local de origem.

Filtros de origem

Os filtros permitem limitar os objetos para cópia de arquivo de acordo com determinados tipos e valores especificados.

Tipo de filtro

Há dois tipos de filtros: Incluir e Excluir.

Um filtro de Inclusão copiará os arquivos somente dos objetos da origem da cópia de arquivo que corresponderem aos valores especificados.

Um filtro de Exclusão copiará todos os objetos da origem da cópia de arquivo, exceto aqueles que corresponderem aos valores especificados.

É possível especificar vários filtros na mesma solicitação de cópia de arquivo separando-se cada valor de filtro com uma vírgula.

- Se forem especificados vários filtros de inclusão, os dados serão incluídos na cópia de arquivo se qualquer um desses filtros for correspondente.
- Se forem especificados vários filtros de exclusão, os dados serão excluídos da cópia de arquivo se qualquer um desses filtros for correspondente.
- É possível misturar filtros de inclusão e exclusão na mesma solicitação de cópia de arquivo.

Observação: quando os parâmetros especificados dos filtros de Inclusão e Exclusão estiverem em conflito, o filtro de Exclusão terá sempre uma prioridade mais alta e será aplicado. Um filtro de Inclusão nunca pode copiar o arquivo de um objeto que também foi excluído.

Variável de filtro (padrão)

Há dois tipos de padrão variável de filtros: padrão de arquivo e padrão de pasta

É possível usar um filtro Padrão de arquivo ou Padrão de pasta para incluir ou excluir determinados objetos da cópia de arquivo.

Valor do filtro

O valor do filtro permite limitar as informações de arquivo copiado selecionando-se apenas as informações de parâmetro especificadas, como arquivos .txt.

O CA ARCserve D2D oferece suporte ao uso de caracteres curinga para ajudar a selecionar vários objetos para cópia de arquivo com uma única solicitação. Um caractere curinga é um caractere especial que pode ser usado como um substituto para representar um único caractere ou uma sequência de caracteres de texto.

Há suporte para o asterisco dos caracteres curinga e para o ponto de interrogação no campo Valor. Se não souber preencher o valor padrão do arquivo/pasta, basta simplificar os resultados do filtro especificando um caractere curinga.

- "*" -- Use o asterisco para substituir zero ou mais caracteres no valor.
- "?" -- Use o ponto de interrogação para substituir um único caractere no valor.

É possível, por exemplo, digitar *.txt para excluir todos os arquivos com uma extensão .txt se não souber o nome do arquivo específico. Pode-se fornecer o máximo de nome de arquivo que souber, use curingas para preencher os espaços em branco.

Observação: quando você seleciona Padrão de arquivo como o tipo de filtro, uma lista suspensa de filtros predefinidos para muitos arquivos normalmente usados é disponibilizada (arquivos MS-Office, arquivos de imagem, arquivos executáveis, arquivos temp. etc.).

Filtro de tamanho de arquivo (apenas tarefas de Cópia de arquivo - excluir origem)

Este filtro aplica-se somente às tarefas Cópia de arquivo - Excluir origem (não às tarefas de cópia de arquivo).

Os filtros de tamanho de arquivo permitem limitar os objetos de origem para cópia de arquivo com base no tamanho do arquivo. Quando você ativa o filtro de tamanho do arquivo, os parâmetros especificados se tornam o filtro para os objetos que serão ou não incluídos na cópia de arquivo. É possível selecionar o intervalo (igual ou maior que, igual ou menor que, ou entre) e digitar um valor para o tamanho.

Por exemplo, se for especificado um valor igual ou maior que 10 MB, o CA ARCserve D2D fará cópia de arquivo apenas de objetos que atendam a esses critérios. Todos os outros objetos que não atenderem aos critérios de tamanho de arquivo não terão cópia de arquivo.

Filtro de tempo de vida de arquivo (apenas tarefas de Cópia de arquivo - excluir origem)

Este filtro aplica-se somente às tarefas Cópia de arquivo - Excluir origem (não às tarefas de cópia de arquivo).

Os filtros de tempo de vida de arquivo permitem incluir automaticamente objetos de origem para cópia de arquivo com base em determinadas datas do arquivo. É possível selecionar um parâmetro (arquivos não acessados em, não modificados em e/ou não criados em) e digitar um valor para o número de dias, meses ou anos do filtro de tempo de vida de arquivo. É possível selecionar vários filtros de tempo de vida de arquivo para cópia de arquivo automática.

Por exemplo, se você especificar Arquivos não modificados em 180 dias, o CA ARCserve D2D copiará automaticamente todos os arquivos que atenderem a esses critérios (não tiverem sido modificados durante os últimos 180 dias).

Importante! Se você especificar os filtros Tamanho do arquivo e Tempo de vida de arquivo (ou vários filtros Tempo de vida de arquivo), somente os arquivos que atenderem a todos os parâmetros de filtro especificados terão cópia de arquivo. Os arquivos que não atenderem a nenhum dos parâmetros especificados não terão cópia de arquivo.

Especificar destinos de cópia de arquivo

O Gerenciador do CA ARCserve Central Protection permite especificar as configurações de destino para que suas informações sejam copiadas em arquivo.

Para especificar destinos de cópia de arquivo

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação.

   A tela Diretivas é exibida.

2. Clique em Novo para criar uma diretiva.

   A caixa de diálogo Nova diretiva é aberta.

3. Selecione a guia Definições da cópia de arquivo e, em seguida, selecione Destino para abrir a caixa de diálogo Destino das definições da cópia de arquivo.

4. Especifique as configurações de destino.

   - **Destino--**especifica o local de destino para a tarefa de cópia de arquivo. Só é possível selecionar um destino.

     O CA ARCserve D2D permite especificar as configurações para cópia dos arquivos armazenados em backup em um disco ou na nuvem. Para a cópia de arquivo, é possível especificar a realização da tarefa copiar e reter ou copiar e mover os dados armazenados para um backup. Os dois processos são semelhantes, com exceção de que, ao executar uma tarefa de copiar e mover, os dados são movidos da origem ao destino (excluídos do local de origem), fornecendo mais espaço livre disponível em sua origem. Ao executar uma cópia e manter, os dados são copiados da origem ao destino (permanece no destino de origem) e fornece várias versões armazenadas.

     − **Cópia de arquivo em uma unidade local ou da rede--**quando selecionada, essa opção permite especificar o caminho completo do local em que deseja mover ou copiar os arquivos e pastas de origem. É possível procura este local de destino. Clicar no ícone de seta verde permite validar a conexão com o destino especificado.

     − **Cópia de arquivo na nuvem--**quando selecionada, essa opção permite especificar o local da nuvem em que deseja mover ou copiar os arquivos e pastas de origem. O CA ARCserve D2D atualmente oferece suporte à cópia de vários fornecedores de nuvem, como Amazon S3 (Simple Storage Service), Windows Azure, Fujitsu Cloud (Windows Azure) e Eucalyptus-Walrus. Esses fornecedores de nuvem são serviços web disponíveis ao público que permitem armazenar e recuperar com segurança qualquer quantidade de dados, a qualquer momento, de qualquer lugar na web.

       Pode-se clicar no botão Configurar para exibir a caixa de diálogo Configuração de nuvem. Para obter mais informações, consulte Especificar os detalhes da configuração de nuvem para cópia de arquivo (na página 110).

       Observação: para eliminar um possível erro de precisão do relógio ao tentar se conectar à nuvem, verifique se o computador tem o fuso horário adequado definido e se o relógio está em sincronia com o tempo global. É necessário verificar sempre a hora de computador referente a hora GMT. Se a hora do computador não estiver sincronizada com o tempo global adequado (de 5 a 10 minutos), o Amazon S3 não funcionará. Se necessário, redefina a hora correta do computador e execute novamente a tarefa cópia de arquivo.

     Para a opção de destino, se a conexão com o destino especificado for perdida ou interrompida, o CA ARCserve D2D fará várias tentativas para continuar a tarefa de cópia de arquivo. Se essas novas tentativas não forem bem-sucedidas, uma tarefa de constituição será executada do ponto em que a falha ocorreu. Além disso, o log de atividades será atualizado com uma mensagem de erro correspondente e uma notificação por email será enviada (se configurada).

- **Compactação--**especifica o tipo de compactação a ser usado para tarefas de cópia de arquivo.

  Em geral, a compactação é executada para reduzir de espaço de armazenamento, mas também tem um impacto inverso sobre a velocidade da cópia de arquivo devido ao aumento no uso da CPU.

  As opções disponíveis são:

  - **Sem compactação**--não será executada nenhuma compactação. Essa opção exige menos uso da CPU (mais velocidade), mas também requer mais espaço de armazenamento para a cópia de arquivo.
  - **Compactação padrão**--alguma compactação será executada. Esta opção proporciona um bom equilíbrio entre o uso da CPU e o requisito do espaço de armazenamento. Essa é a configuração padrão.
  - **Compactação máxima**--a compactação máxima será executada. Essa opção exige mais uso da CPU (menos velocidade), mas também requer menos espaço de armazenamento para a cópia de arquivo.

- **Criptografia--**permite ativar a senha de criptografia para a cópia de arquivo.

- **Tempo de retenção--**esta configuração se aplica apenas aos dados copiados do arquivo que foram movidos (não os que foram retidos).

  Especifica o tempo (anos, meses, semanas, dias) que os dados armazenados são retidos no local de destino. No final do período de retenção especificado, os dados armazenados serão removidos do destino.

  Os cálculos do tempo de retenção tem como base um mês de 30 dias e um ano de 365 dias. Por exemplo: se você especificar um período de retenção de 2 anos, 2 meses e 5 dias, o período total de retenção para os dados do arquivo copiado será de 795 dias (365 + 365 + 30 + 30 + 5).

  Importante: Em virtude da configuração do tempo de retenção se aplicar apenas aos dados copiados e movidos da origem para o destino (e não copiados e retidos), é importante entender que ao final do período de retenção especificado, em que os dados são eliminados do destino, todos estes dados movidos não serão mais armazenados ou salvos.

- **Versões do arquivo--**esta configuração se aplica apenas a dados copiados que foram retidos (não os que foram movidos).

  Especifica o número de cópias mantidas e armazenadas no local de destino (nuvem ou disco). Quando este número for excedido, a primeira versão (mais antiga) será descartada. O ciclo de descartar a versão armazenada mais antiga será repetido à medida que versões mais novas forem adicionadas ao destino, permitindo que você sempre mantenha a quantidade especificada de versões armazenadas.

  Por exemplo, se a contagem de retenção de versões de arquivo especificada for definida como 5 e se você fizer cinco cópias de arquivo nas horas t1, t2, t3, t4 e t5, estas se tornarão as cinco versões de cópia de arquivo retidas e disponíveis para recuperação. Depois que a sexta cópia do arquivo foi executada (a versão nova foi salva), o CA ARCserve D2D removerá a cópia t1 e as cinco versões disponíveis para recuperação agora são t2, t3, t4, t5 e t6.

  Por padrão, a quantidade de cópias mantida no local de destino antes de descartar é 15.

5. Clique em Salvar configurações.

As configurações de destino da cópia de arquivo são salvas.

Especificar os detalhes da configuração de nuvem para a cópia de arquivo

Nessa caixa de diálogo, é possível usar o menu suspenso para selecionar o tipo de fornecedor da nuvem que deseja usar para armazenar as cópias de arquivo. As opções disponíveis são Amazon S3, Windows Azure, Fujitsu Cloud (Windows Azure) e Eucalyptus-Walrus. (Amazon S3 é o fornecedor padrão). Para obter mais informações sobre a Fujitsu Cloud (Windows Azure), consulte a Visão geral e registro.

Observação: se estiver usando o Eucalyptus-Walrus como seu fornecedor da nuvem de cópia de arquivo, não será possível copiar arquivos cujo tamanho de caminho total excede 170 caracteres.

As opções de configuração para cada fornecedor da nuvem são semelhantes (com algumas terminologias distintas), e nenhuma diferença é descrita.

1. Especificar as definições de conexão:

   URL do fornecedor

   Identifica o endereço URL do provedor da nuvem.

   (Para Amazon S3, Windows Azure e a Fujitsu Cloud (Windows Azure), o URL do fornecedor é automaticamente preenchido. Para Eucalyptus-Walrus, o URL do fornecedor deve ser inserido manualmente usando o formato especificado).

ID da chave de acesso/nome da conta/ID de consulta

Identifica o usuário que está solicitando acesso a este local.

(Para esse campo, o Amazon S3 usa a ID da chave de acesso. Windows Azure e Fujitsu Cloud (Windows Azure) usam o Nome da conta e a Eucalyptus-Walrus usa a ID de consulta).

Chave de acesso secreta/chave secreta

Uma vez que a chave de acesso não está criptografada, esta chave de acesso secreta será uma senha usada para verificar a autenticidade da solicitação para acessar este local.

Importante: Esta chave de acesso secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave de acesso secreta em uma página da web ou em outro código de origem de acesso público e não a transmita em canais não seguros.

(Para esse campo, o Amazon S3 usa a chave de acesso secreta. Windows Azure, Fujitsu Cloud (Windows Azure) e Eucalyptus-Walrus usam a chave secreta).

Ativar proxy

Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes (nome de usuário e senha) para usar o servidor proxy.

(O recurso proxy não está disponível para Eucalyptus-Walrus).

2. Especificar configurações avançadas:

   Nome do compartimento de memória/Contêiner

   Todos os arquivos e as pastas movidos ou copiados para o fornecedor da nuvem são armazenados e organizados nos compartimentos de memória (ou contêineres). Os compartimentos de memória são como um contêiner para os arquivos e são usados para agrupar e organizar objetos. Cada objeto armazenado no fornecedor da nuvem é colocado em um compartimento de memória.

   (Para esse campo, o Amazon S3 e Eucalyptus-Walrus usam o Nome do compartimento de memória. Windows Azure e Fujitsu Cloud (Windows Azure) usam Contêiner).

   Observação: para o restante desta etapa, todas as referências a compartimentos de memória também podem ser aplicadas aos recipientes, contanto que seja especificado.

Para especificar um novo nome do compartimento de memória:

a. Especifique o novo nome do compartimento de memória.

   Observação: o Gerenciador do CA ARCserve Central Protection não cria o nome do compartimento de memória. No entanto, é gerado para cada nó do CA ARCserve D2D quando uma diretiva do Gerenciador do CA ARCserve Central Protection é atribuída com êxito. O Nome do compartimento de memória para cada nó do CA ARCserve D2D é prefixado automaticamente com "d2dfilecopy-<hostname>-<user given name>".

   O nome de um compartimento de memória é exclusivo, facilmente identificável e em conformidade com as regras de nomenclatura de domínio da internet. Dois compartimentos de memória não podem ter o mesmo nome. É importante compreender a sintaxe válida para nomes de compartimento de memória.

   Para Amazon S3 e Eucalyptus-Walrus, consulte a documentação do Amazon S3 para obter mais informações sobre os requisitos de nomenclatura do compartimento de memória.

   Para Windows Azure e Fujitsy Cloud (Windows Azure), consulte a documentação da Microsoft para obter mais informações sobre requisitos de nomenclatura do contêiner.

b. Para Amazon S3 somente, selecione uma região disponível no menu suspenso. Por padrão, todas as regiões disponíveis serão incluídas no menu suspenso e é possível selecionar a região onde deseja que o novo compartimento de memória seja criado.

   As regiões permitem escolher a região geográficas onde o Amazon S3 irá armazenar os compartimentos de memória criados. É necessário selecionar uma Região que ofereça acesso rápido aos seus dados e permita otimizar a latência, reduzir os custos ou abordar solicitações regulatórias.

   (Para Windows Azure, Fujitsu Cloud (Windows Azure) e Eucalyptus-Walrus, a região não pode ser selecionada).

c. Após especificar valores, clique em OK. O nome do compartimento de memória será validado e criado na nuvem.

d. Após criar o compartimento de memória com êxito, a caixa de diálogo principal Configuração de nuvem é exibida novamente com as novas informações do compartimento de memória (nome e uma região) incluídas no campo Configurações avançadas.

Ativar a redução de armazenamento de dados redundantes

Para Amazon S3 apenas, esta opção permite ativar a RRS (Reduced Redundancy Storage). A RRS é uma opção de armazenamento no Amazon S3 que ajuda a reduzir os custos, armazenando dados reproduzíveis, não críticos em níveis de redundância mais baixos do que o armazenamento padrão do Amazon S3. As opções de armazenamento padrão e de redução de armazenamento de dados redundantes armazenam dados em vários recursos e dispositivos, mas com a RRS os dados são replicados menos vezes e o custo é menor. Deve-se esperar a mesma latência e taxa de transferência usando o armazenamento padrão ou RRS do Amazon S3. Por padrão, esta opção não está selecionada (o Amazon S3 usa a opção de armazenamento padrão).

3. Clique em Testar conexão para verificar a conexão com o local na nuvem especificado.
4. Clique em OK para sair da caixa de diálogo Configuração de nuvem.

Especificar programações da cópia de arquivo

O Gerenciador do CA ARCserve Central Protection permite especificar as configurações de programação para que suas informações sejam copiadas em arquivo.

Para programações de cópia de arquivo

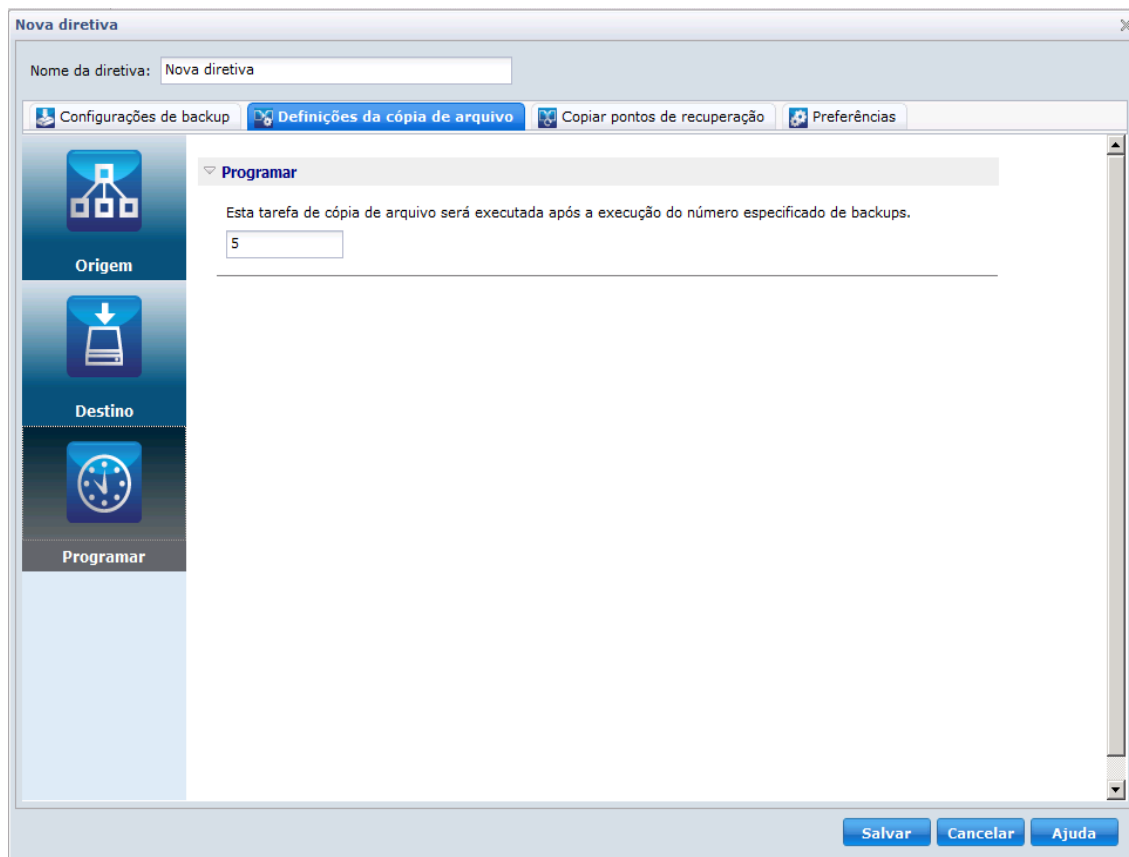
1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação.

   A tela Diretivas é exibida.

2. Clique em Novo para criar uma diretiva.

   A caixa de diálogo Nova diretiva é aberta.

3. Selecione a guia Definições da cópia de arquivo e, em seguida, selecione Programação.

   A caixa de diálogo Programação das definições da cópia de arquivo é exibida.

4. Especifique as configurações da programação da cópia de arquivo.

   - **Programar--**permite a cópia de dados do arquivo após o número especificado de backups.

     O processo de cópia de arquivo será iniciado automaticamente após o número especificado de backups realizados com êxito e será de acordo com as diretivas de cópia de arquivo selecionado.

     É possível usar esta configuração para controlar o número de vezes que uma tarefa de cópia de arquivo será disparada a cada dia. Por exemplo, se especificar a execução de uma tarefa de backup a cada 15 minutos, e a execução de uma tarefa de cópia de arquivo após cada 4 backups, haverá 24 cópias de arquivo em execução todos os dias (1 por hora).

     Por padrão, a programação para a cópia de arquivo ocorre após a conclusão de cada cinco backups realizados com êxito. (O número máximo de backups que pode ser especificado é 700).

5. Clique em Salvar configurações.

As configurações de programação de cópia de arquivo são salvas.

Especifique as configurações da cópia de pontos de recuperação

O CA ARCserve D2D permite especificar as configurações de programação para os pontos de recuperação a serem copiados (e exportados, se necessário). Para entender melhor o uso das opções desta caixa de diálogo para configurar a programação da cópia de ponto de recuperação, consulte o tópico Copiar pontos de recuperação - cenários de exemplo.

Observação: o processo de copiar ponto de recuperação é uma operação de copiar e colar apenas e não uma operação de recortar e colar. Como resultado, sempre que uma tarefa de cópia de ponto de recuperação programada for executada, o CA ARCserve D2D cria uma cópia adicional do ponto de recuperação no destino de cópia especificado, enquanto mantém a cópia original do ponto de recuperação no destino de backup especificado em Configurações de backup.

Para especificar as configurações da cópia de pontos de recuperação

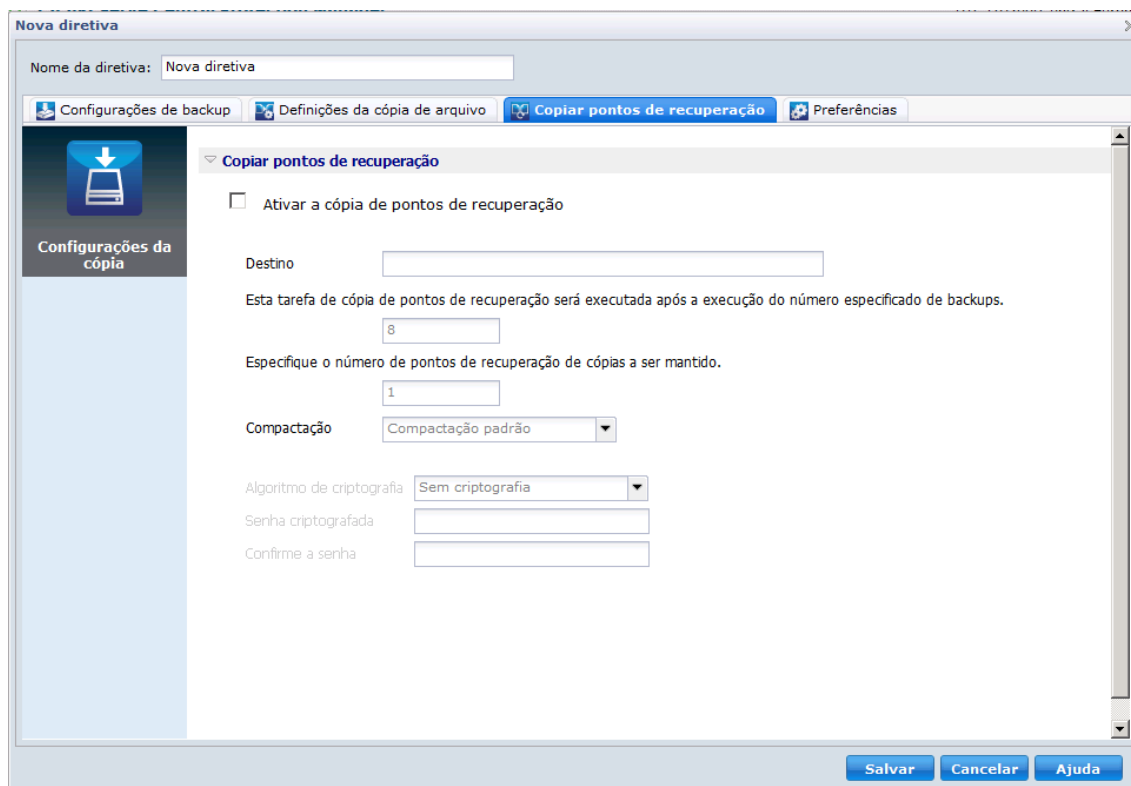
1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação.

   A tela Diretivas é exibida.

2. Clique em Novo para criar uma diretiva.

   A caixa de diálogo Nova diretiva é aberta.

3. Selecione a guia Copiar pontos de recuperação.

   A caixa de diálogo Copiar pontos de recuperação é exibida.

4. Especifique as configurações da programação da cópia de ponto de recuperação.

   Ativar a cópia de pontos de recuperação

   Ativa a cópia de pontos de recuperação programada após o número especificado de backups. Se essa opção não estiver marcada, nenhuma cópia de pontos de recuperação programada será executada.

   Destino

   Especifica o local (destino) para a cópia dos pontos de recuperação ou é possível procurar um local para a cópia. Clique no botão de ícone de seta verde para verificar a conexão com o local especificado.

A tarefa Copiar pontos de recuperação será executada após a quantidade especificada de backups realizada.

Especifica quando o processo de cópia de ponto de recuperação programado será iniciado automaticamente.

O processo de cópia de ponto de recuperação será iniciado automaticamente após o número especificado de backups realizados com êxito e terá como base as diretivas de cópia selecionadas.

É possível usar esta configuração para controlar o número de vezes que um processo de cópia de ponto de recuperação será disparado a cada dia. Por exemplo, se especificar a execução de uma tarefa de backup a cada 15 minutos, determine que a cópia dos pontos de recuperação seja executada a cada 4 backups, assim, haverá 24 tarefas de cópia de ponto de recuperação executadas a cada dia (1 por hora).

Por padrão, a programação para a cópia de ponto de recuperação será realizada após cada oito backups concluídos com êxito.

Importante! Se as tarefas de cópia e backup forem programadas para serem executadas em intervalos regulares e se a tarefa de cópia estiver em execução no momento (em estado ativo) em que a hora programada para a tarefa de backup chegar, esta tarefa irá falhar. (A próxima tarefa de backup será executada conforme programada e deve ser bem-sucedida se não estiver em conflito com outra tarefa de cópia). Uma vez que a operação de cópia leva quase o mesmo tempo que a execução de um backup completo, a melhor prática é definir uma programação frequente para as tarefas de cópia de ponto de recuperação.

Especificar a quantidade de pontos de cópia de recuperação a serem mantidos.

Especifica a quantidade de pontos de recuperação mantidos e armazenados no destino de cópia especificado. Quando este número for excedido, o primeiro (o mais antigo) ponto de recuperação será descartado. O ciclo de descartar os pontos de recuperação mais antigos se repetirá à medida que pontos de recuperação mais recentes forem adicionados ao destino, permitindo manter sempre o número especificado de pontos de recuperação armazenados.

Observação: se o destino não tiver espaço livre suficiente, considere reduzir a quantidade de pontos de recuperação salva.

Por padrão, a contagem de retenção é definida como 31 pontos de recuperação.

Observação: o número máximo de pontos de recuperação é 1344.

Compactação

Especifica o tipo de compactação a ser usada para cópias de ponto de recuperação.

A compactação geralmente é executada para reduzir o uso do espaço em disco, mas também tem um impacto adverso na velocidade do backup devido ao aumento do uso da CPU.

As opções disponíveis são:

- **Sem compactação** - a compactação não será executada. Os arquivos estão no formato VHD puro. Essa opção exige menos uso da CPU (mais velocidade), mas também mais uso de espaço em disco para a imagem de backup.
- **Sem compactação - VHD** - a compactação não será executada. Os arquivos são convertidos para o formato .vhd diretamente, sem a necessidade de operações manuais. Essa opção exige menos uso da CPU (mais velocidade), mas também mais uso de espaço em disco para a imagem de backup.
- **Compactação padrão** - alguma compactação será executada. Essa opção proporciona um bom equilíbrio entre o uso da CPU e o uso do espaço em disco. Essa é a configuração padrão.
- **Compactação máxima** - a compactação máxima será executada. Essa opção proporciona maior uso da CPU (menos velocidade), mas também menos uso de espaço em disco para a imagem de backup.

Observação: se a imagem de backup contiver dados não compactáveis (como imagens JPG ou arquivos ZIP), espaço adicional de armazenamento poderá ser alocado para lidar com esses dados. Como resultado, se você selecionar qualquer opção de compactação e possuir dados não compactáveis no backup, ele pode na verdade resultar em um aumento do uso de espaço em disco.

Algoritmo de criptografia

Especifique o tipo de algoritmo de criptografia a ser usado para as cópias de ponto de recuperação.

A criptografia de dados é a conversão de dados em uma forma ininteligível sem um mecanismo decodificador. A proteção de dados do CA ARCserve D2D usa algoritmos de criptografia seguros AES (padrão de criptografia avançada) para atingir o máximo de segurança e privacidade dos dados especificados.

As opções de formatação são Sem criptografia, AES-128, AES-192 e AES-256. (Para desativar criptografia, selecione Sem criptografia.)

Senha criptografada

Se o ponto de recuperação a ser copiado foi anteriormente criptografado, será necessário fornecer (e confirmar) a senha.

- Se o ponto de recuperação estiver sendo copiado para um local no mesmo computador, a senha criptografada será lembrada e este campo será automaticamente preenchido.
- Se o ponto de recuperação estiver sendo copiado para outro computador, será necessário digitar a senha criptografada.

5. Clique em Salvar configurações.

As configurações da cópia de ponto de recuperação são salvas.

Gerenciar preferências

O Gerenciador do CA ARCserve Central Protection permite que você gerencie as necessidades gerais de uma diretiva. Você pode gerar novos feeds ou criar notificações de alertas por email ou atualizar o servidor ou as conexões.

Esta seção contém os seguintes tópicos

Especificar Preferências gerais

O Gerenciador do CA ARCserve Central Protection permite gerenciar as preferências gerais de uma diretiva.

Para especificar preferências gerais

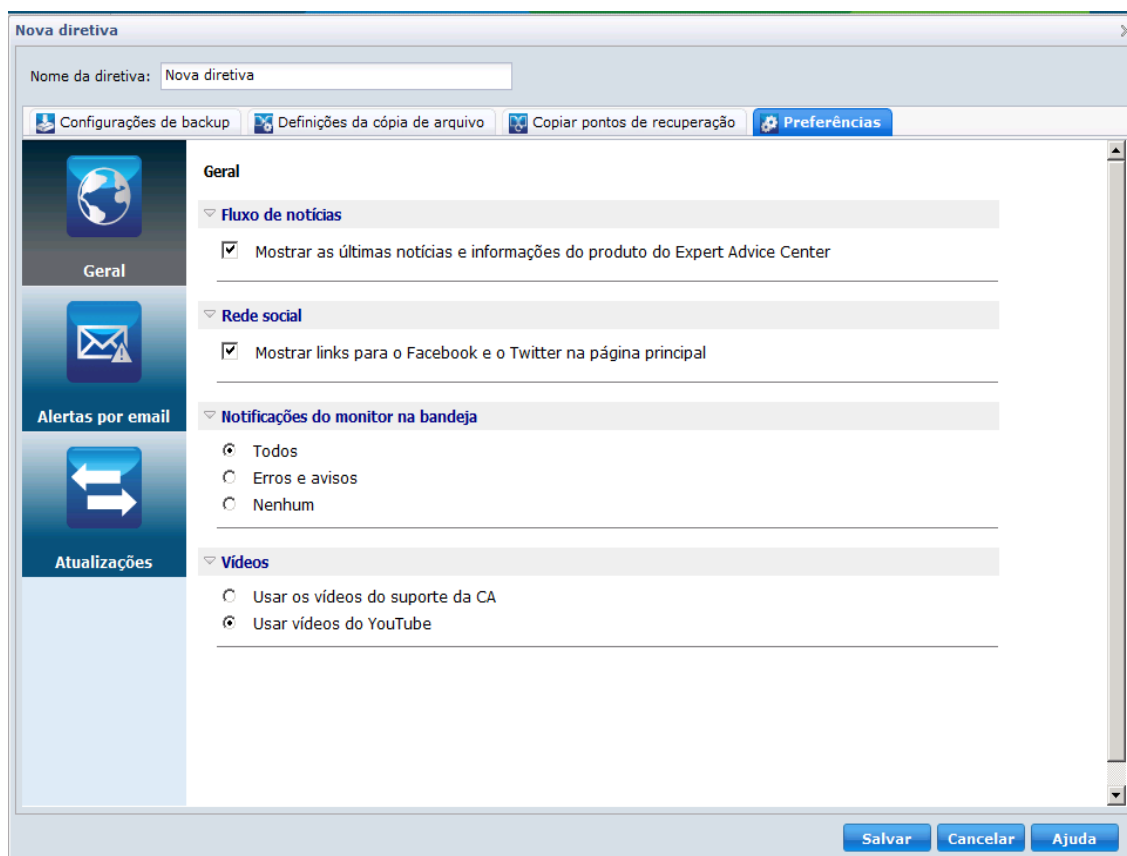
1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação.

   A tela Diretivas é exibida.

2. Clique em Novo para criar uma diretiva.

   A caixa de diálogo Nova diretiva é aberta.

3. Selecione a guia Preferências.

   A caixa de diálogo Preferências gerais é aberta.

4. Especifique suas preferências

   - **Feed de notícias--**ative esta opção para exibir as últimas notícias e informações do produto a partir do Expert Advice Center.
   - **Rede social--**ative esta opção para exibir links para o Facebook e Twitter na página principal.
   - **Notificações da bandeja--**selecione uma das seguintes opções:
     - Selecione Tudo para exibir todas as notificações na bandeja do sistema.
     - Selecione Erros e avisos para exibir apenas erros e avisos na bandeja do sistema.
     - Selecione Nenhum para não exibir notificações.
   - **Vídeos--**selecione um dos tipos de vídeo para usar na diretiva do D2D:
     - Usar os vídeos do suporte da CA
     - Usar vídeos do YouTube (padrão)

5. Clique em Salvar.

As preferências gerais são salvas.

Especificar alertas por email

O Gerenciador do CA ARCserve Central Protection permite especificar preferências de Alertas por email.

Para especificar alertas por email

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação.

   A tela Diretivas é exibida.

2. Clique em Novo para criar uma diretiva.

   A caixa de diálogo Nova diretiva é aberta.

3. Selecione a guia Preferências e, em seguida, selecione Alertas por email.

   A caixa de diálogo Preferências de alertas por email é aberta.

4. Especifique os alertas por email.

   - **Ativar o envio de alertas por email--**selecione esta opção para ativar as preferências nesta tela.

   - **Configurações de email--**clique neste botão para abrir a caixa de diálogo Configurações de email. (na página 124)

   - **Notificações--**especifica o envio automático de notificações de alerta por email após a conclusão dos eventos selecionados. Você pode selecionar qualquer uma ou todas as opções disponíveis.

     As opções disponíveis permitem enviar uma notificação de alerta para os seguintes eventos:

     Alertas de tarefas de backup

     - **Tarefas não executadas--**envia uma notificação de alerta por email para todas as tarefas não executadas. Uma tarefa não executada é qualquer tarefa programada que não tenha sido executada conforme a programação. Isso pode ocorrer quando alguma outra tarefa está em execução ou uma tarefa anterior que começou mais cedo ainda não tiver terminado. Por exemplo, se uma tarefa de exportação ou recuperação estiver em execução na hora programada para uma tarefa de backup, então, a tarefa de backup não será executada.

     - **Falha/paralização de tarefas de backup, catálogo, cópia de arquivo, restauração ou cópia de ponto de recuperação**--envia uma notificação de alerta por email para todas as tentativas sem êxito de tarefas de backup, catálogo, cópia de arquivo, restauração ou cópia de ponto de recuperação. Esta categoria inclui todas as tentativas com falha, incompletas, canceladas e paralisadas, bem como as tarefas não executadas.

- **Êxito em tarefas de backup, catálogo, cópia de arquivo, restauração ou cópia de ponto de recuperação--**envia uma notificação de alerta por email para todas as tentativas bem-sucedidas de tarefas de backup, catálogo, cópia de arquivo, restauração ou cópia de ponto de recuperação.
- **A tarefa de mesclagem foi interrompida, com falha ou paralisada** -- envia uma notificação de alerta para todas as tarefas de mesclagem interrompidas, ignoradas, com falha ou paralisadas. Se você não ativar este alerta, você será informado toda vez que houver falha na mesclagem da tarefa. Pode ocorrer uma falha na mesclagem devido às seguintes razões: a sessão está montada, a sessão está bloqueada por uma tarefa de catálogo ou a sessão está bloqueada por outra razão.
- **Tarefa de mesclagem com êxito** -- envia um alerta a cada tarefa de mesclagem bem-sucedida.

Alertas de espaço em disco

- **O espaço livre do destino de backup é menor que**--envia uma notificação de alerta por email quando a quantidade de espaço não utilizado no destino de backup for menor do que um valor especificado. Para esta opção, pode-se ainda selecionar a porcentagem da capacidade total ou um valor específico (em MB) para o nível do limite de quando uma notificação de alerta deve ser enviada.

Alertas de atualização

- **Há atualizações disponíveis**--envia uma notificação por email quando uma nova atualização do CA ARCserve D2D estiver disponível. Notificações por email também serão enviadas quando ocorrer uma falha durante a verificação de atualizações ou durante o download.

Alertas do recurso

- **Ativar alertas do recurso--**envia uma notificação por email quando o nível de limite do principal indicador de desempenho (PKI) especificado for atingido. Para garantir que o servidor seja eficiente e confiável, é necessário monitorar continuamente o desempenho para identificar possíveis problemas e tratar rapidamente as situações de gargalo.

  Definir níveis de limite para esses indicadores de desempenho é estritamente a seu critério e de seus conhecimentos sobre o servidor. Não há configurações certas ou erradas e as notificações de alerta devem ter como base desempenho normal e aceitável. Por exemplo, se o sistema normalmente é executado em uma carga da CPU de 80%, então definir um limite de 75% da utilização da CPU não será muito útil ou eficiente.

  Cada um desses parâmetros de PKI podem ser separadamente configurados para enviar uma notificação de alerta quando o nível de limite correspondente for atingido. O número máximo de emails de alerta de PKI que será enviado será de 5 por dia.

- **Utilização da CPU**--o limite de alerta especificado indica a porcentagem de utilização da CPU para o servidor protegido do CA ARCserve D2D. Você pode usar esta notificação de alerta para certificar-se de que o servidor não fique sobrecarregado com muita frequência.

  Se o uso da CPU for muito alto, o tempo de resposta do servidor pode se tornar muito lento ou parar de responder e a divisão (equilíbrio) da carga deverá ser considerada.

- **Taxa de transferência de disco**--o limite de alerta especificado indica a taxa de transferência do disco (MB/segundo) para o servidor protegido do CA ARCserve D2D. Você pode usar esta notificação de alerta para certificar-se de que está maximizando a capacidade do disco.

  Se a taxa de transferência do disco estiver próxima ao valor máximo que o disco pode suportar, deve-se considerar a atualização para um disco que atenda melhor às suas necessidades. Geralmente, um disco mais rápido resulta em um melhor desempenho.

- **Utilização da memória**--o limite de alerta especificado indica o percentual de utilização da memória no servidor protegido do CA ARCserve D2D. Utilização refere-se a quanto da capacidade da memória está sendo usada. Quanto maior a porcentagem, pior será o desempenho do servidor.

  Se o uso da memória for muito intenso de forma contínua, é necessário determinar qual processo está causando esse alto uso. Você pode usar esta configuração do indicador para alertá-lo quando uma atualização de aplicativo ou de servidor pode ser necessária.

- **E/S de rede**--o limite de alerta especificado indica o percentual de largura de banda da NIC que você está usando no momento no servidor protegido do CA ARCserve D2D. A utilização refere-se a quanto da capacidade da interface de rede (ou NIC) está sendo usada. Quanto maior a porcentagem, pior será o desempenho da rede.

Se o uso da rede for muito intenso, será necessário determinar qual processo está causando esse alto uso e corrigir o problema. Além disso, se, com base na capacidade de rede específica, a porcentagem de utilização da rede estiver muito alta durante o horário do backup, talvez seja necessário atualizar sua placa NIC para atender aos requisitos de maior taxa de transferência.

5. Clique em Salvar.

As opções de alerta por email são salvas.

Especificar as configurações de email

A caixa de diálogo Configurações de email preenche automaticamente os valores atuais do servidor de email e a configuração da diretiva de email para a nova diretiva. Essas configurações serão aplicadas a todas as notificações de alerta de email e podem ser modificadas a qualquer momento.

Serviço

O serviço do provedor de email a ser usado para enviar notificações de alerta. As opções disponíveis são Google Mail, Yahoo Mail, Live Mail e Outros.

- Se você selecionar Outros, é preciso identificar o servidor de email e o número da porta usado como a configuração padrão.
- Se você selecionar Google Mail, Yahoo Mail ou Live Mail, os campos de servidor de email e número de porta são preenchidos automaticamente.

Servidor de email

O nome de host do servidor de email SMTP que o CA ARCserve D2D pode usar para enviar os alertas por email.

Porta

O número da porta de saída para o servidor de email.

Requer autenticação

Especifica se esse servidor de email exige autenticação ao tentar enviar um email pela internet. Quando essa opção é selecionada, é preciso fornecer o nome da conta e a senha correspondentes.

Assunto

Descrição de um assunto para as notificações de alerta que o CA ARCserve D2D enviará por email. Por padrão, a descrição é Alerta do CA ARCserve D2D.

De

O endereço de email que o CA ARCserve D2D usará para enviar as notificações de alerta por email.

Destinatários

Endereço de email para os destinatários que recebem as notificações de alerta por email.

Observação: para digitar vários endereços de email, separe-os usando ponto e vírgula.

Use o recurso Seleção automática do SSL

O servidor de email requer uma conexão SSL (Secure Sockets Layer) para transmitir dados com segurança pela internet.

Enviar STARTTLS

O servidor de email requer a emissão de um comando STARTTLS (extensão Start TLS) para iniciar uma conexão SMTP segura entre servidores.

Usar formato HTML

As notificações de alerta serão enviadas em formato HTML por email. Se essa opção não for selecionada, os alertas serão enviados como texto sem formatação. Por padrão, esta opção está ativada.

Ativar configurações de proxy

Especifica se você deseja conectar-se a um servidor proxy para enviar suas notificações de alerta por email. Quando essa opção for selecionada, o nome do servidor proxy e o número de porta correspondentes devem ser fornecidos.

Email de teste

Verifica se as configurações de email estão corretas.

Especificar Preferências de atualização

O Gerenciador do CA ARCserve Central Protection permite especificar suas preferências de atualização.

Para especificar as preferências de atualização

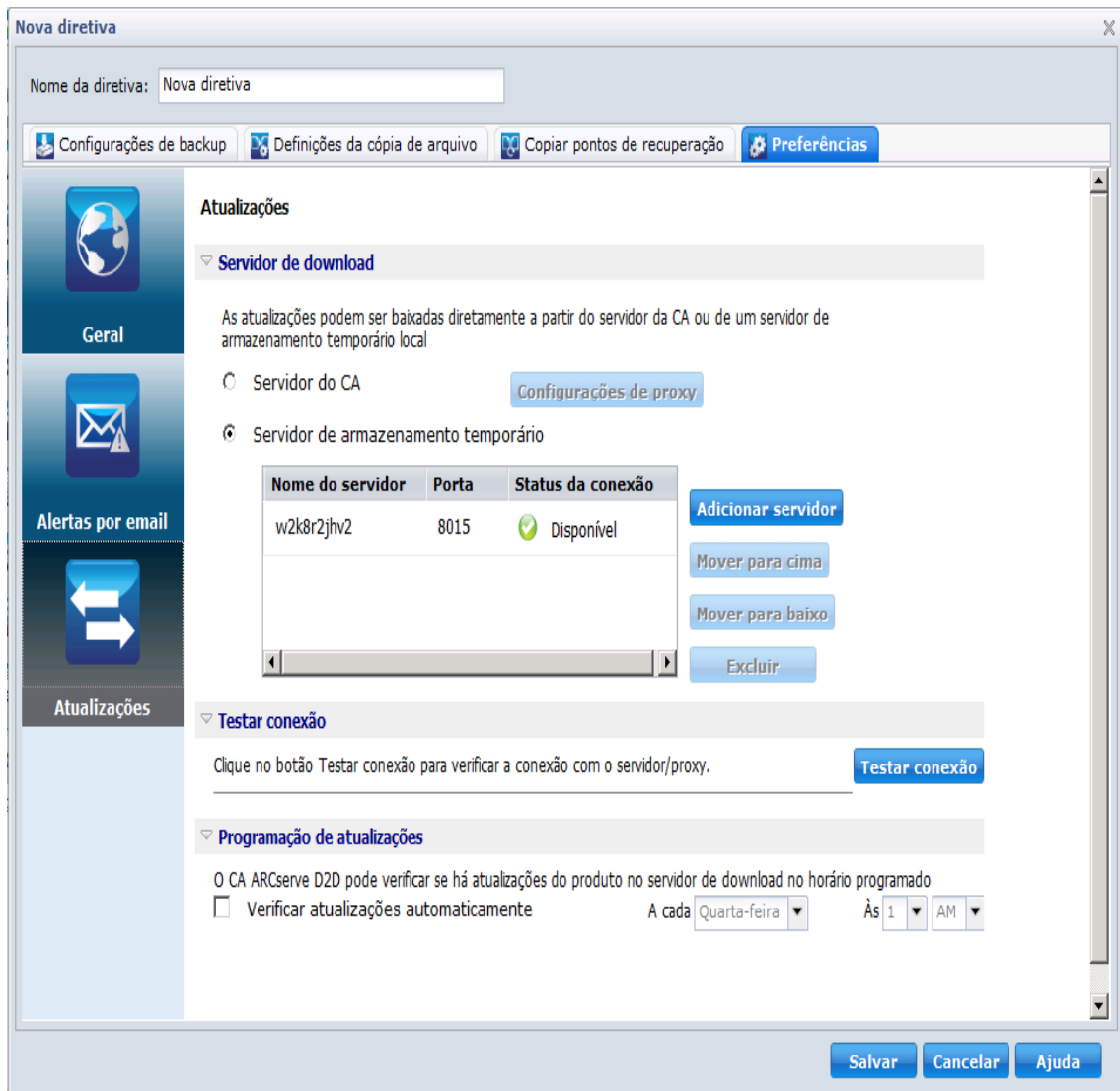
1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação.

   A tela Diretivas é exibida.

2. Clique em Novo para criar uma diretiva.

   A caixa de diálogo Nova diretiva é aberta.

3. Selecione a guia Preferências e, em seguida, selecione Atualizar.

   A caixa de diálogo Atualização de preferências é aberta.

4. Especifique suas preferências de atualização.

   - **Servidor de download--**especifica o servidor de origem a partir do qual o servidor do CA ARCserve D2D estabelecerá conexão e fará download das atualizações disponíveis.

     – **Servidor da CA Technologies--**use esta opção para especificar que as atualizações do CA ARCserve D2D devem ser baixadas do servidor da CA Technologies diretamente para o servidor local.

     – **Servidor de armazenamento temporário**--Use essa opção para especificar o servidor que deseja usar como armazenamento temporário.

       Se você especificar mais de um servidor de armazenamento temporário, o primeiro servidor listado será designado como o servidor principal de armazenamento temporário. O CA ARCserve D2D tentará inicialmente se conectar ao servidor de armazenamento temporário principal. Se, por qualquer motivo, o primeiro servidor listado não estiver disponível, o próximo servidor listado se tornará o servidor de armazenamento temporário principal. A mesma sequência será seguida até que o último servidor listado se torne o servidor de armazenamento temporário principal. (A lista de servidores de armazenamento temporário está limitada ao máximo de 5 servidores.)

     – Você pode usar os botões Mover para cima e Mover para baixo para alterar a sequência de servidores de armazenamento temporário.

     – Você pode usar o botão Excluir para remover um servidor desta listagem.

     – Você pode usar o botão Adicionar servidor para adicionar um novo servidor a esta listagem. Ao clicar no botão Adicionar servidor, a caixa de diálogo Servidor de armazenamento temporário é exibida, permitindo que você especifique o nome do servidor de armazenamento temporário adicionado e o número da porta cujo padrão é o número de porta atual.

       Essa é a configuração padrão.

       Observação: para as diretivas do D2D, o servidor de armazenamento temporário padrão é o computador local do CA ARCserve Central Applications.

       As atualizações do CA ARCserve D2D serão baixadas do servidor da CA Technologies diretamente para o servidor de armazenamento temporário especificado. Depois que as atualizações forem baixadas para o servidor de armazenamento temporário, você pode obter o download das atualizações a partir do servidor de armazenamento temporário para um servidor cliente. Se selecionar o local do servidor de armazenamento temporário, especifique o nome do host ou o endereço IP do servidor de armazenamento temporário, juntamente com o número de porta correspondente.

■ **Configurações de proxy--**este recurso está disponível apenas quando o servidor da CA está selecionado como o servidor de download.

Clique em Configurações de proxy para especificar se deseja que as atualizações do CA ARCserve D2D sejam baixadas por meio de um servidor proxy. Esta será a conexão com o servidor da CA a partir do qual o servidor de download obterá as atualizações.

Quando você clicar neste botão, a caixa de diálogo Configurações de proxy será aberta.

– **Usar configurações de proxy do navegador (apenas para IE e Chrome)--**permite usar as credenciais fornecidas para o proxy do CA ARCserve D2D.

– **Especificar configurações proxy--**o servidor proxy atua como um intermediário entre o servidor de download (de armazenamento temporário ou cliente) e o servidor da CA para garantir a segurança, o desempenho e o controle administrativo. Por padrão, essa opção é desativada.

Selecione essa opção para usar um servidor proxy para se conectar ao CA server a fim de obter informações de atualização do CA ARCserve D2D. O servidor proxy se conectará diretamente ao servidor da CA para obter informações de atualização. Com esta opção ativada, inclua o endereço IP (ou nome do host) do servidor proxy e o número da porta correspondente que é usada pelo servidor proxy em conexões com a internet.

Se você não selecionar essa opção, o servidor de download se conectará diretamente ao servidor da CA sem um servidor proxy.

Além disso, você também pode especificar se o servidor proxy requer autenticação. Quando selecionado, especifica que as informações de autenticação (ID e senha do usuário) são obrigatórias para usar o servidor proxy.

- **Testar conexão**--permite testar as conexões abaixo e exibir uma mensagem de status mediante a conclusão:
  - Se você selecionou Servidor da CA Technologies como o servidor de download, ele testa a conexão entre o computador e o servidor da CA Technologies por meio do servidor proxy especificado.
  - Se você selecionou Servidor de armazenamento temporário como o servidor de download, ele testa a conexão entre o computador e o servidor da CA Technologies por meio do servidor de armazenamento temporário especificado.

    O botão Testar conexão é usado para testar a disponibilidade de cada servidor de armazenamento temporário listado e um status correspondente é exibido no campo Status de conexão.

  Observação: o teste de conexão é executado automaticamente quando abrir a caixa de diálogo Preferências de atualizações automáticas ao criar uma diretiva.

- **Programação de atualizações--**especifica quando verificar (e fazer download) de novas atualizações do CA ARCserve D2D.

  Com esta opção selecionada, ele verifica automaticamente atualizações novas e disponíveis do CA ARCserve D2D. Caso selecione essa opção, haverá recursos de menu suspenso para especificar quando executar essa função (todos os dias ou semanalmente em um dia especificado) e a hora do dia na qual ela será executada.

  Se você selecionar esta opção e não especificar um dia e horário, o agendamento padrão deverá executar a verificação automática todo domingo às 04:00.

  Por padrão, se essa verificação determinar que uma nova atualização está disponível, o CA ARCserve D2D fará download da atualização automaticamente. Se não desejar baixar automaticamente as atualizações, é possível desativar essa função no arquivo D2DPMSettings.INI. Para obter mais informações, consulte o Guia do Usuário do CA ARCserve D2D no site de CA Support https://support.ca.com/cadocs/0/CA%20ARCserve%20D2D%20r16-ENU/Bookshelf.html.

Se você não selecionar essa opção, ele desativa todas as funções automáticas de verificação e download (e seu status é exibido na seção de Resumo do status da página inicial).

Essas funções de atualização só podem ser iniciadas manualmente.

Observação: se for configurado, você receberá uma notificação por email se a verificação agendada para atualizações detectar que uma nova atualização está disponível. Além disso, as notificações por email também serão enviadas quando ocorrer uma falha durante a verificação de atualizações ou durante o download.

5. Clique em Salvar.

As preferências atualizadas são salvas.

Editar ou copiar diretivas

O Gerenciador do CA ARCserve Central Protection permite editar e copiar diretivas depois de serem criadas.

Para editar diretivas

1. Efetue logon no aplicativo.

   Clique em Diretivas na barra de navegação para abrir a tela Diretivas.

2. Na tela Diretivas, clique na caixa de seleção ao lado de uma diretiva e execute uma das seguintes ações:

   - Clique em Editar na barra de ferramentas e edite a diretiva selecionada.
   - Clique em Copiar na barra de ferramentas para copiar e criar uma nova diretiva a partir da diretiva selecionada.

     Observação: ao copiar uma diretiva, a caixa de diálogo Copiar diretiva é aberta. Especifique um nome para o nova diretiva e clique em OK.

   A caixa de diálogo Editar diretiva é aberta.

3. Se desejar alterar o nome da diretiva, especifique um nome no campo Nome da diretiva.

4. Especifique os valores necessários e clique em Salvar.

A diretiva é editada ou copiada.

Excluir diretivas

O Gerenciador do CA ARCserve Central Protection permite excluir diretivas criadas anteriormente.

Observação: o Gerenciador do CA ARCserve Central Protection não permite que você exclua as diretivas atribuídas a nós. Para excluir diretivas que contêm nós atribuídos, você deve primeiro remover a atribuição de nós da diretiva para depois excluí-la. Para obter informações sobre como remover a atribuição de nós de uma diretiva, consulte o tópico Atribuir e remover atribuição de nós de diretivas (na página 133).

Para excluir diretivas

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação.

   A tela Diretivas é exibida.

2. Na lista de diretivas, clique na diretiva que deseja excluir.

3. Clique em Excluir na barra de ferramentas de Diretivas.

   Uma mensagem de confirmação de exclusão é exibida.

4. Clique em Sim para excluir a diretiva.

   Observação: se você excluir uma diretiva por engano, será necessário recriá-la. Se você não deseja excluir a diretiva, clique em Não.

A diretiva é excluída.

Implantar diretivas

O Gerenciador do CA ARCserve Central Protection permite implantar diretivas independentemente de ter sido implantado várias vezes ou não ter sido implantado em servidores remotos.

Para implantar diretivas

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação

   A tela Diretivas é exibida.

2. Selecione uma Diretiva na Lista Diretivas e clique em Implantar agora.

   A diretiva é implantada imediatamente.

Observação: quando a diretiva for implantada com êxito em um nó do CA ARCserve D2D, não é possível alterar todas as configurações no nó do CA ARCserve D2D. Exceto pelo botão ativado Update Connection, o CA ARCserve D2D pode sincronizar as informações de conexão para o destino de backup apenas se as credenciais de acesso tiverem sido alteradas no servidor remoto. Além disso, é possível exibir o status da implantação de diretivas na tela de lista de Nós na coluna Diretivas.

Atribuir e remover a atribuição de nós de diretivas.

O Gerenciador do CA ARCserve Central Protection permite atribuir ou remover a atribuição de nós de diretivas do D2D existentes.

Siga estas etapas:

1. Na página inicial do Gerenciador do CA ARCserve Central Protection, clique em Diretivas na barra de navegação para abrir a tela Diretivas.

2. Selecione uma Diretiva na lista Diretivas e clique na guia Atribuição de diretiva.

   Uma lista de nós atribuídos à diretiva selecionada é exibida com um dos seguintes status e ações de implantação (formato: *[ação] status de implantação*):

   - [Assign] Pendente
   - [Unassign] Implantando
   - [Resync] Concluído
   - [Update] Com falha
   - [Re-deploy] Êxito ao implantar o D2D
   - [Re-deploy] Falha ao implantar o D2D
   - [Re-deploy] Implantar reinicialização do D2D

3. Clique no botão Atribuir e remover atribuição.

   A caixa de diálogo Atribuir/remover atribuição de diretiva é aberta.

4. Especifique os seguintes campos da caixa de diálogo Atribuir/remover a atribuição de diretivas:

   - **Grupo--**permite selecionar o nome do grupo que contém os nós que deseja atribuir.
   - **Filtro Nome do nó--**permite filtrar os nós disponíveis com base em critérios comuns.

     Observação: o campo Nome do nó permite filtrar nós usando caracteres curinga.

     Por exemplo, usar o Acc* permite filtrar todos os nós com um nome de nó que comece com Acc. Para limpar os resultados do filtro, clique em X no campo Filtro.

5. Execute uma das seguintes ações:

   - **Atribuir nós a diretivas--**selecione os nós que deseja adicionar e clique na seta à direita.

     Os nós são movidos da lista Nós disponíveis para a lista Nós selecionados.

     Observação: para selecionar e mover todos os nós, clique na seta dupla à direita.

   - **Remover a atribuição de nós de diretivas**--selecione os nós que deseja remover a atribuição e clique na seta à esquerda.

     Os nós são movidos da lista Nós selecionados para a lista Nós disponíveis.

     Observação: para selecionar e mover todos os nós, clique na seta dupla à esquerda.

   Clique em OK.

   Observação: A seguinte mensagem é exibida ao remover a atribuição de diretivas:

   `Você está removendo a atribuição de diretivas do nó selecionado. É possível manter as configurações atuais para permitir que o nó continue o processo de backup. Deseja manter as configurações? Clique em Sim para manter as configurações atuais do CA ARCserve D2D, clique em Não para remover as configurações atuais do CA ARCserve D2D ou clique em Cancelar para voltar à tela Atribuir e remover a atribuição de diretivas.`

   Se clicar em Não, as configurações remotas do CA ARCserve D2D serão perdidas e o servidor do CA ARCserve D2D não será protegido.

Os nós são aplicados a diretivas especificadas.

Executar um backup agora

Em geral, os backups são executados automaticamente e controlados pelas configurações da programação. No entanto, pode ser necessário executar um backup ad-hoc (completo, incremental ou de verificação) imediatamente.

Um backup ad hoc é realizado conforme necessário, em vez de agendado antecipadamente como parte de um plano de backup. Por exemplo, se você repetir a programação para backups completos, incrementais e de verificação e desejar fazer grandes alterações em seu computador, é possível executar um backup ad hoc imediato sem esperar até que o próximo backup programado ocorra.

Um backup ad hoc permite também adicionar um ponto de recuperação personalizado (não programado) para que seja possível reverter a este ponto anterior no tempo, se necessário. Por exemplo, se um patch ou service pack for instalado e, em seguida, for detectado que ele afeta negativamente o desempenho do computador, talvez você queira reverter para a sessão de backup ad hoc que não inclua o patch ou service pack.

Siga estas etapas:

1. Efetue logon no aplicativo.
2. Na barra de navegação na página inicial, clique em Nó para abrir a tela Nó.
3. Execute uma das seguintes ações para especificar os nós para backup:
   - **Nível de nó:** clique no grupo que contém os nós para backup e, em seguida, clique na caixa de seleção ao lado dos nós para backup.
   - **Nível de grupo:** clique no grupo que contém os nós para backup.
4. Em seguida, execute uma das seguintes ações para fazer backup do nó:
   - Na barra de ferramentas, clique em Backup.
   - Clique com o botão direito do mouse no grupo selecionado ou clique com o botão direito do mouse nos nós e, em seguida, clique em Fazer backup agora no menu de contexto.

5. Na caixa de diálogo Executar um backup agora, especifique o tipo de backup, clicando em um dos seguintes tipos:

   ■ **Backup completo--**inicia um backup completo de todo o computador ou de volumes selecionados.

   ■ **Backup incremental--**inicia um backup incremental do computador. Um backup incremental realiza backup somente dos blocos que foram alterados desde o backup anterior.

     Observação: as vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a execução de backups.

   ■ **Backup de verificação--**inicia um backup de verificação do computador, examinando o backup mais recente de cada bloco e comparando o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup para algum bloco não corresponder à origem, o CA ARCserve D2D atualizará (nova sincronização) o backup do bloco de dados que não corresponder. Considere as seguintes vantagens e desvantagens para executar backups de verificação:

     − Vantagens - uma imagem de backup muito pequena é produzida quando comparada ao backup completo porque somente os blocos alterados (blocos que não correspondam ao último backup) são armazenados em backup.

     − Desvantagens - o backup é mais demorado porque todos os blocos do disco de origem são comparados aos blocos do último backup.

   Observação: se você adicionar um novo volume à origem do backup, será feito um backup completo do volume recém-adicionado, independentemente do método de backup geral selecionado.

6. (Opcional) Especifique o Nome do backup e clique em OK. Se você não especificar um nome, ele será nomeado por padrão como Backup personalizado/completo/incremental/de verificação.

Uma tela de confirmação é exibida, e o tipo de backup selecionado é iniciado imediatamente.

Esteja ciente do seguinte:

■ Todos os valores especificados nas caixas de diálogo Diretiva são aplicados à tarefa.

■ Se houver falha em uma tarefa de backup personalizada (ad hoc), nenhuma tarefa de constituição será criada. Uma tarefa de constituição pode ser criada apenas para tarefas programadas com falha.

Exibir informações de status da tarefa

Quando uma tarefa estiver em execução, você poderá exibir informações detalhadas sobre ela. Como alternativa, você pode interromper uma tarefa em andamento.

Siga estas etapas:

1. Efetue logon no aplicativo.
2. Na barra de navegação na página inicial, clique em Nó para abrir a tela Nó.
3. Na árvore Grupos, clique no grupo que contém o nó do qual deseja exibir o status da tarefa.

   Se a tarefa estiver em andamento, a fase da tarefa será exibida na coluna Tarefa.

4. Clique na fase na coluna Tarefa para abrir a caixa de diálogo Monitor de status de backup.
5. Na caixa de diálogo Monitor de status de backup, você pode fazer o seguinte:
   - Clique em Fechar para fechar a caixa de diálogo Monitor de status de backup.
   - Clique em Cancelar para interromper a tarefa atual.

     Observação: a caixa de diálogo Monitor de status de backup será fechada imediatamente depois de clicar em Cancelar.

Como restaurar nós no Gerenciador do CA ARCserve Central Protection

O Gerenciador do CA ARCserve Central Protection fornece várias ferramentas e opções que podem ser usadas para restaurar dados. Este capítulo inclui informações sobre como restaurar dados de forma segura e eficiente.

A seção contém os seguintes tópicos:

Restaurar dados de pontos de recuperação

Procurar pontos de recuperação permite restaurar quaisquer aplicativos navegando até os pontos de recuperação disponíveis (backups bem-sucedidos) em uma visualização de calendário.

Para restaurar dados de pontos de recuperação

1. Efetue logon no aplicativo e clique em Nó na barra de navegação.
2. Na tela Nó, expanda o grupo que contém o nó que deseja restaurar.

   Clique na caixa de seleção ao lado do nó que deseja restaurar e, em seguida, clique em Restaurar na barra de ferramentas.
3. Na caixa de diálogo Restaurar, clique em Procurar pontos de recuperação.

   A caixa de diálogo Procurar pontos de recuperação é exibida.
4. Especifique o Local de backup ou procure o local onde as imagens de backup estão armazenadas.

   Observação: clique na seta verde próximo ao botão Procurar para validar a conexão com o destino de backup especificado. Pode ser necessário inserir as credenciais de nome de usuário e senha para se conectar a um compartilhamento de rede remoto.

   A visualização do calendário realçará em verde todas as datas do período exibido que contiverem os pontos de recuperação para essa origem de backup.
5. Especifique as informações para restaurar.
   a. Selecione a data no calendário para a imagem de backup que deseja restaurar.

      Os pontos de recuperação correspondentes a essa data são exibidos, juntamente com a hora do backup, o tipo de backup que foi executado, o nome do backup e o status do catálogo.
   b. Selecione o ponto de recuperação que deseja restaurar.

      O conteúdo do backup correspondente (incluindo aplicativos) para esse ponto de recuperação é exibido.
   c. Selecione o conteúdo a ser restaurado.
      - Para uma restauração em nível de volume, pode-se especificar a restauração do volume inteiro ou de arquivos ou pastas selecionados no volume.
      - Para uma restauração de nível de aplicativo, é possível especificar a restauração do aplicativo inteiro ou de itens selecionados no aplicativo, como componentes, bancos de dados, instâncias e assim por diante.

   Clique em Avançar.

   A caixa de diálogo Opções de restauração é exibida.

6. Selecione o destino da restauração.

   As opções disponíveis são restaurar no local original do backup ou restaurar em um local diferente.

   Restaurar no local original

   Restaura no local original a partir do qual a imagem de backup foi capturada.

   Observação: ao restaurar a pasta de logs do CA ARCserve D2D no local original, os arquivos que estiverem nessa pasta serão ignorados. Para o CA ARCserve Central Host-Based VM Backup esta opção é desativada por padrão. Para usá-la, instale o CA ARCserve D2D dentro do SO convidado e, em seguida, faça a restauração.

   Restaurar em:

   É possível especificar um local ou procurar o local em que as imagens de backup serão restauradas. Clique no botão de ícone de seta verde para verificar a conexão com o local especificado.

   Se necessário, você precisará digitar as credenciais de nome de usuário e senha para obter acesso a esse local.

7. Selecione a opção sobre como o CA ARCserve D2D pode resolver conflitos encontrados durante o processo de restauração.

   As opções disponíveis são:

   Substituir arquivos existentes

   Substitui (sobrescreve) qualquer arquivo localizado no destino da restauração. Todos os objetos serão restaurados nos arquivos de backup, independentemente da presença atual deles em seu computador.

   Substituir os arquivos ativos

   Substitui todos os arquivos ativos ao reinicializar. Se, durante a tentativa de restauração, o CA ARCserve D2D detectar que o arquivo existente está atualmente em uso ou sendo acessado, ele não substituirá o arquivo imediatamente, mas evitará que qualquer problema atrase a substituição dos arquivos ativos até a próxima reinicialização do computador. (A restauração ocorrerá imediatamente, mas a substituição de arquivos ativos é feita durante a reinicialização seguinte.)

Observação: se essa opção não estiver selecionada, os arquivos ativos serão ignorados na restauração.

Renomear arquivos

Cria um novo arquivo se o nome de arquivo já existir. A seleção desta opção copia o arquivo de origem no destino com o mesmo nome de arquivo, mas com uma extensão diferente. Os dados serão restaurados no novo arquivo.

Ignorar arquivos existentes

Ignora e não substitui (sobrescreve) os arquivos localizados no destino da restauração. Apenas os objetos inexistentes em seu computador no momento serão restaurados dos arquivos de backup.

Por padrão, esta opção está ativada.

8. (Opcional) Selecione Criar diretório raiz em Estrutura de diretórios.

   Isso permite ao CA ARCserve D2D recriar a mesma estrutura de diretórios raiz no caminho de destino da restauração.

   Observação: se essa opção não for selecionada, o arquivo ou pasta a ser restaurado será restaurado diretamente para a pasta de destino.

9. Digite a senha de criptografia de backup para restaurar os dados criptografados e, em seguida, clique em Avançar.

   A caixa de diálogo Resumo da restauração é exibida.

10. Examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.

    - Se as informações de resumo não estiverem corretas, clique em Anterior e volte à caixa de diálogo em questão para alterar a configuração incorreta.

Se as informações de resumo estiverem corretas, clique em Concluir para iniciar o processo de restauração.

Restaurar dados de cópias de arquivo

A opção Procurar cópias de arquivo permite recuperar dados de cópias dos arquivos do CA ARCserve D2D. Cópias dos arquivos são cópias de pontos de recuperação do CA ARCserve D2D que você copia para o armazenamento offline, como um disco ou a nuvem. Usando as cópias dos arquivos, você pode especificar os dados que deseja recuperar.

Para restaurar dados de cópias de arquivo

1. Efetue logon no aplicativo e clique em Nó na barra de navegação.
2. Na tela Nó, expanda o grupo que contém o nó que deseja restaurar.

   Clique na caixa de seleção ao lado do nó que deseja restaurar e, em seguida, clique em Restaurar na barra de ferramentas.

3. Na caixa de diálogo Restaurar, clique em Procurar cópias de arquivo.

   A caixa de diálogo Procurar cópias de arquivo é exibida.

4. No painel Nome, especifique os dados da cópia de arquivo que você deseja recuperar. É possível especificar qualquer combinação de arquivos e pastas ou o volume.

   Quando você selecionar um arquivo individual para restauração, todas as versões do arquivo copiado serão exibidas no painel à direita. Se várias versões estiverem disponíveis, selecione a versão de cópia do arquivo que deseja recuperar.

   - **Alterar--** permite procurar um local alternativo no qual as imagens de cópias de arquivos serão armazenadas.

     Uma caixa de diálogo é exibida, mostrando as opções alternativas de destino disponíveis.

     - **Unidade local ou de rede -** a caixa de diálogo Selecione um local de backup é aberta, permitindo procurar e selecionar uma unidade local ou de rede diferente.
     - **Nuvem -** a caixa de diálogo Configuração de nuvem é aberta, permitindo acessar e selecionar um local de nuvem diferente.

5. Clique em Avançar.

   A caixa de diálogo Opções de restauração é aberta.

6. Preencha as seguintes opções na caixa de diálogo Opções de restauração:

   - **Destino -** selecione o destino da restauração.

     – Restaurar no local original - permite restaurar dados no local original do qual a imagem de backup foi capturada.

     – Restaurar para - permite especificar ou procurar o local em que as imagens de backup serão restauradas. Clique na seta ao lado do campo Restaurar para de forma a verificar a conexão com o local especificado.

       Se necessário, você precisará digitar as credenciais de nome de usuário e senha para obter acesso a esse local.

- **Resolvendo conflitos -** permite especificar como o CA ARCserve D2D deve resolver conflitos encontrados durante o processo de restauração.
  - Substituir os arquivos existentes - permite substituir arquivos existentes que estão localizados no destino de restauração. Todos os objetos serão restaurados nos arquivos de backup, independentemente da presença atual deles em seu computador.
  - Substituir arquivos ativos - permite substituir os arquivos ativos na reinicialização. Se a tentativa de restauração do CA ARCserve D2D detectar que o arquivo existente está em uso, ele não substituirá o arquivo imediatamente. Em vez disso, para evitar problemas, ele atrasará a substituição dos arquivos ativos até a próxima reinicialização do computador. (A restauração ocorrerá imediatamente, mas a substituição de arquivos ativos é feita durante a reinicialização seguinte.)

    Observação: se essa opção não estiver selecionada, os arquivos ativos serão ignorados na restauração.
  - Renomear arquivos - permite criar novos arquivos se o nome de arquivo já existir. A seleção desta opção copia o arquivo de origem no destino com o mesmo nome de arquivo, mas com uma extensão diferente. Os dados serão, então, restaurados no novo arquivo.
  - Ignorar arquivos existentes - permite ignorar e não substituir arquivos existentes localizados no destino da restauração. Apenas os objetos inexistentes em seu computador no momento serão restaurados dos arquivos de backup.

    Por padrão, esta opção está ativada.
- **Estrutura de diretórios -** permite especificar o que o CA ARCserve D2D fará ou não com a estrutura de diretórios durante o processo de restauração.
  - Criar diretório raiz - permite especificar que, se uma estrutura de diretório raiz existir na imagem de backup capturada, o CA ARCserve D2D recriará a mesma estrutura de diretórios raiz no caminho de destino da restauração.

    Quando a opção Criar diretório raiz não estiver selecionada (desmarcada), o arquivo/pasta a ser restaurado será restaurado diretamente na pasta de destino.

    Exemplo:

    Se, durante o backup, você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt" e "C:\Pasta1\Subpasta2\B.txt" e, durante a restauração, foi especificado como destino de restauração o local "D:\Restore".

    Se você optar por restaurar os arquivos "A.txt" e "B.txt" individualmente, o destino dos arquivos restaurados será "D:\Restore\A.txt" e "D:\Restore\B.txt" (o diretório raiz acima do nível de arquivo especificado não será recriado).

Se você optar por restaurar a partir do nível da "Subpasta2", o destino dos arquivos restaurados será "D:\Restore\Subpasta2\A.txt" e "D:\Restore\Subpasta2\B.txt" (o diretório acima do nível de pasta especificado não será recriado).

Quando a opção Criar diretório raiz estiver selecionada (marcada), todo o caminho do diretório raiz até os arquivos/pastas (incluindo o nome do volume) será recriado na pasta de destino. Se os arquivos/pastas a serem restaurados forem do mesmo nome de volume, o caminho do diretório raiz de destino não incluirá esse nome de volume. No entanto, se os arquivos/pastas a serem restaurados forem de nomes de volume diferentes, o caminho do diretório raiz do destino incluirá o nome do volume.

Exemplo:

Se, durante o backup, você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt", "C:\Pasta1\Subpasta2\B.txt" e "E:\Pasta3\Subpasta4\C.txt" e, durante a restauração, foi especificado como destino de restauração o local "D:\Restauração".

Se você optar por restaurar apenas o arquivo "A.txt", o destino do arquivo restaurado será "D:\Restore\Pasta1\Subpasta2\A.txt" (o diretório raiz inteiro, sem o nome do volume, será recriado).

Se você optar por restaurar tanto o arquivo "A.txt" quanto o "C.txt", o destino dos arquivos restaurados será "D:\Restore\C\Pasta1\Subpasta2\A.txt" e "D:\Restore\E\Pasta3\Subpasta4\C.txt" (o diretório raiz inteiro, com o nome do volume, será recriado).

- **Senha criptografada -** se os dados do ponto de recuperação que você está tentando restaurar estiverem criptografados, poderá ser necessário fornecer a senha criptografada.

  A senha não será obrigatória caso esteja tentando restaurar no computador em que o backup criptografado foi executado. No entanto, caso esteja tentando restaurar em um computador diferente, a senha será necessária.

  Observação: os ícones a seguir indicam se o ponto de recuperação contém informações criptografadas e poderá exigir uma senha para restauração.

  Ponto de recuperação não criptografado (ícone do relógio):

  Ponto de recuperação criptografado (ícone do relógio com cadeado):

Clique em Avançar.

A caixa de diálogo Resumo de restauração é exibida.

7. Verifique se as informações na caixa de diálogo Resumo da restauração estão corretas.

   Observação: para alterar as opções de restauração especificadas, clique em Voltar e retorne à caixa de diálogo aplicável para alterar os valores.

   Clique em Concluir.

As opções de restauração são aplicadas e os dados são recuperados.

Restaurar dados de arquivos e pastas

Sempre que o aplicativo executar um backup com êxito, todas as pastas ou arquivos armazenados em backup serão incluídos na imagem de instantâneo do seu backup. Este método de restauração permite especificar exatamente qual arquivo ou pasta deve ser restaurado.

Para restaurar dados de arquivos e pastas

1. Efetue logon no aplicativo e clique em Nó na barra de navegação.

   Na tela Nó, expanda o grupo que contém o nó que deseja restaurar.

   Clique na caixa de seleção ao lado do nó que deseja restaurar e, em seguida, clique em Restaurar na barra de ferramentas.

2. Na caixa de diálogo Restaurar, clique em Localizar arquivos/pastas para restauração.

   A caixa de diálogo Localizar arquivos/pastas para restauração é exibida.

3. Especifique o Local de backup e o Local de cópia de arquivo ou procure o local onde as imagens de backup estão armazenadas.

   Esteja ciente do seguinte:

   - Para o Local de backup, clique na seta verde próximo ao botão Procurar para validar a conexão com o destino de backup especificado. Pode ser necessário inserir as credenciais de nome de usuário e senha para se conectar a um compartilhamento de rede remoto.

   - Para Local de cópia de arquivo, é possível clicar no botão Alterar para um local ou unidade de rede ou para a nuvem. Para obter mais detalhes sobre Local da cópia de arquivo, consulte Restaurar dados de cópias de arquivo (na página 140).

4. Especifique o nome de arquivo ou pasta para restaurar.

   Observação: o campo Nome de arquivo oferece suporte à pesquisa de nome completo e pesquisa com caracteres curinga. Se não souber o nome do arquivo completo, é possível simplificar os resultados da pesquisa especificando os caracteres curinga "*" e "?" no campo Nome de arquivo.

   Os caracteres curinga suportados para o nome de arquivo ou pasta são os seguintes:

   - "*" - use o asterisco para substituir zero ou mais caracteres em um nome de arquivo ou diretório.
   - "?" - use o ponto de interrogação para substituir um único caractere em um nome de arquivo ou pasta.

   Por exemplo, se *.txt for especificado, todos os arquivos com uma extensão de arquivo .txt serão exibidos nos resultados da pesquisa.

5. (Opcional) Especifique um nome de caminho para refinar sua pesquisa e selecione se deseja incluir ou não subdiretórios ou arquivos e pastas.

6. Clique em Localizar para iniciar a pesquisa.

   Os resultados da pesquisa são exibidos. Se a pesquisa detectar várias ocorrências (pontos de recuperação) do mesmo arquivo pesquisado, ela listará todas as ocorrências classificadas por data (com a mais recente listada primeiro).

7. Selecione a versão que deseja restaurar da lista e clique em Avançar.

   A caixa de diálogo Opções de restauração é exibida.

8. Selecione o destino da restauração.

   As opções disponíveis são restaurar no local original do backup ou restaurar em um local diferente.

   Restaurar no local original

   Restaura no local original a partir do qual a imagem de backup foi capturada.

   Observação: ao restaurar a pasta de logs do CA ARCserve D2D no local original, os arquivos que estiverem nessa pasta serão ignorados.

   Restaurar em:

   É possível especificar um local ou procurar o local em que as imagens de backup serão restauradas. Clique no ícone de seta verde para verificar a conexão com o local especificado.

   Se necessário, você precisará digitar as credenciais de nome de usuário e senha para obter acesso a esse local.

9. Selecione a opção sobre como o CA ARCserve D2D pode resolver conflitos encontrados durante o processo de restauração.

   As opções disponíveis são:

   Substituir arquivos existentes

   Substitui (sobrescreve) qualquer arquivo localizado no destino da restauração. Todos os objetos serão restaurados nos arquivos de backup, independentemente da presença atual deles em seu computador.

   Substituir os arquivos ativos

   Substitui todos os arquivos ativos ao reinicializar. Se, durante a tentativa de restauração, o CA ARCserve D2D detectar que o arquivo existente está atualmente em uso ou sendo acessado, ele não poderá substituir o devido arquivo imediatamente. Para evitar problemas, adiará a substituição dos arquivos ativos até a próxima reinicialização do computador. (A restauração ocorrerá imediatamente, mas a substituição de arquivos ativos é feita durante a próxima reinicialização).

   Observação: se essa opção não estiver selecionada, os arquivos ativos serão ignorados na restauração.

   Renomear arquivos

   Cria um novo arquivo se o nome de arquivo já existir. A seleção desta opção copia o arquivo de origem no destino com o mesmo nome de arquivo, mas com uma extensão diferente. Os dados serão restaurados no novo arquivo.

   Ignorar arquivos existentes

   Ignora e não substitui (sobrescreve) os arquivos localizados no destino da restauração. Apenas os objetos inexistentes em seu computador no momento serão restaurados a partir dos arquivos de backup.

   Por padrão, esta opção está ativada.

10. (Opcional) Selecione Criar diretório raiz em Estrutura de diretórios.

    Isso permite ao CA ARCserve D2D recriar a mesma estrutura de diretórios raiz no caminho de destino da restauração.

    Observação: se essa opção não for selecionada, o arquivo ou pasta a ser restaurado será restaurado diretamente para a pasta de destino.

11. Digite a senha de criptografia de backup para restaurar os dados criptografados e, em seguida, clique em Avançar.

    A caixa de diálogo Resumo da restauração é exibida.

12. Examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.

    ■ Se as informações de resumo não estiverem corretas, clique em Anterior e volte à caixa de diálogo em questão para alterar a configuração incorreta.

Se as informações de resumo estiverem corretas, clique em Concluir para iniciar o processo de restauração.

Restaurar dados de máquinas virtuais

Use a opção Restaurar VM (máquina virtual) para restaurar uma máquina virtual cujo backup tenha sido feito anteriormente.

Para restaurar dados de máquinas virtuais

1. Efetue logon no aplicativo e clique em Nó na barra de navegação.

   Na tela Nó, expanda o grupo que contém o nó que deseja restaurar.

   Clique na caixa de seleção ao lado do nó que deseja restaurar e, em seguida, clique em Restaurar na barra de ferramentas.

2. Na caixa de diálogo Restaurar, clique em Recuperar VM.

   A caixa de diálogo Restaurar é exibida.

3. Especificar o local do backup (origem). Você pode especificar um local ou procurar o local onde as suas imagens de backup estão armazenadas. Se necessário, forneça as credenciais de nome de usuário e senha para acessar esse local. Pode-se clicar no ícone de validação em forma de seta verde para confirmar o devido acesso ao local de origem.

   A exibição do calendário realçará (em verde) todas as datas do período exibido que contiverem os pontos de recuperação para essa origem de backup.

4. Especifique a máquina virtual a ser restaurada.

   O menu suspenso incluirá todas as máquinas virtuais no local de backup especificado.

5. Selecione a data no calendário para a imagem da máquina virtual que deseja restaurar.

   Os pontos de recuperação correspondentes a essa data são exibidos, juntamente com a hora do backup, o tipo de backup que foi executado e o nome do backup.

6. Selecione o ponto de recuperação que deseja restaurar.

   O conteúdo do backup correspondente (incluindo aplicativos) para esse ponto de recuperação é exibido apenas para referência. Ao restaurar uma máquina virtual, todo o computador será restaurado. Como resultado, é possível exibir, mas não selecionar volumes, pastas ou arquivos individuais a partir da máquina virtual selecionada.

   Observação: um ícone de relógio com um símbolo de cadeado indica que o ponto de recuperação contém informações criptografadas e que pode ser necessária uma senha para restaurar.

7. Quando as informações do backup a ser restaurado forem especificadas, clique em Avançar.

   A caixa de diálogo Opções de restauração é exibida.

8. Selecione o destino da restauração.

   Restaurar no local original

   Restaura a máquina virtual no local original a partir do qual a imagem de backup foi capturada. Por padrão, esta opção está ativada.

   Para obter mais informações, consulte o tópico Restaurar a VM no local original.

   Restaurar em um local diferente.

   Restaura a máquina virtual em outro local de onde a imagem de backup foi capturada.

   Para obter mais informações, consulte o tópico Restaurar a VM em um local diferente.

9. Especifique o que o CA ARCserve D2D deve fazer para resolver os conflitos encontrados durante o processo de restauração.

   A opção disponível destina-se a substituir a máquina virtual existente. Por padrão, essa opção de substituição não está selecionada.

   - Caso tenha selecionado essa opção, o processo de restauração substitui (sobrescreve) quaisquer imagens existentes desta máquina virtual que estiverem localizadas no destino de restauração determinado. A imagem da máquina virtual é restaurada dos arquivos de backup, independentemente de sua presença atual no destino da restauração.
   - Se esta opção não for selecionada, o processo de restauração cria uma imagem separada desta máquina virtual que não substitui nenhuma imagem existente localizada no destino da restauração especificada.

10. Marque a opção Após a recuperação.

    Selecione se o consumo de energia será aplicado à máquina virtual no final do processo de restauração. Por padrão, essa opção de ligar não está selecionada.

Restaurar máquinas virtuais aos locais originais

Durante o processo de configuração para restaurar a VM, é necessário selecionar a opção de onde deseja restaurá-la. As seleções disponíveis são Restaurar no local original e Restaurar em um local diferente.

Se selecionar restaurar a VM no local original, execute as seguintes etapas:

Para restaurar máquinas virtuais aos locais originais

1. Na caixa de diálogo Opções de restauração, após especificar as opções Resolver conflitos e Após a recuperação, selecione Restaurar para o local original e clique em Avançar.

   Observação: para obter mais informações sobre as opções Resolver conflitos e Após a recuperação, consulte o tópico Restaurar dados de máquinas virtuais (na página 147).

   A caixa de diálogo Definir credencial para a origem vCenter/ESX Server é exibida.

2. Especifique as credenciais para acessar a máquina virtual.

   - **vCenter/ESX Server--**especifique o nome do host ou endereço IP de destino do sistema vCenter ou ESX Server.
   - **Nome da VM--**especifique o nome de host da máquina virtual que você está restaurando.
   - **Protocolo--**especifique o protocolo que deseja usar para a comunicação com o servidor de destino. As seleções disponíveis são HTTP e HTTPS.
   - **Número da porta--**especifique a porta que deseja usar para a transferência de dados entre o servidor de origem e o destino. Por padrão, este número da porta é 443.
   - **Nome de usuário**--especifique o nome de usuário com permissão de acesso para efetuar logon na máquina virtual que você está restaurando.
   - **Senha--**especifique a senha correspondente para o nome de usuário necessária para fazer logon na máquina virtual que está restaurando.

3. Quando as credenciais forem especificadas, clique em OK.

   A caixa de diálogo Resumo de restauração é exibida.

4. Examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.

   - Se as informações de resumo não estiverem corretas, clique em Anterior e volte à caixa de diálogo em questão para alterar a configuração incorreta.
   - Se as informações de resumo estiverem corretas, clique em Concluir para iniciar o processo de restauração.

Restaurar máquinas virtuais para locais diferentes

Durante o processo de configuração para restaurar a VM, é necessário selecionar a opção de onde deseja restaurá-la. As seleções disponíveis são Restaurar no local original e Restaurar em um local diferente.

Se desejar restaurar a máquina virtual em um local alternativo, execute as seguintes etapas:

Para restaurar máquinas virtuais para locais diferentes

1. Na caixa de diálogo Opções de restauração, após marcar as opções Resolver conflitos e Após a recuperação, selecione Restaurar em um local diferente.

   Observação: para obter mais informações sobre as opções Resolver conflitos e Após a recuperação, consulte o tópico Recuperar dados em máquinas virtuais (na página 147).

   A caixa de diálogo Opções de restauração se expande para exibir restauração adicional em opções diferentes.

2. Especifique as informações do vCenter/ESX Server.

   - **vCenter/ESX Server--**especifique o nome do host ou endereço IP de destino do sistema vCenter ou ESX Server.
   - **Nome de usuário**--especifique o nome de usuário com permissão de acesso para efetuar logon na máquina virtual que estiver restaurando.
   - **Senha--**especifique a senha correspondente para o nome de usuário necessária para fazer logon na máquina virtual que está restaurando.
   - **Protocolo--**especifique o protocolo que deseja usar para a comunicação com o servidor de destino. As seleções disponíveis são HTTP e HTTPS.
   - **Número da porta--**especifique a porta que deseja usar para a transferência de dados entre o servidor de origem e o destino. Por padrão, este número da porta é 44.

3. Quando as informações do vCenter/ESX Server estiverem especificadas, clique no botão Estabelecer conexão com esse vCenter/ESX Server.

   Se as informações de credenciais de acesso ao servidor alternativo estiverem corretas, os campos Outras informações ficarão ativados.

4. Especificar outras informações.

   - **Nome da VM--**especifique o nome de host da máquina virtual que você está restaurando.
   - **ESX Server--**especifique o servidor ESX de destino. O menu suspenso contém uma lista de todos os servidores ESX associados à máquina virtual especificada.
   - **Armazenamento de dados da VM**--especifica o armazenamento de dados da VM de destino.

5. Quando outras informações forem especificadas, clique em Avançar.

   A caixa de diálogo Resumo de restauração é exibida.

6. Examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.

   - Se as informações de resumo não estiverem corretas, clique em Anterior e volte à caixa de diálogo em questão para alterar a configuração incorreta.
   - Se as informações de resumo estiverem corretas, clique em Concluir para iniciar o processo de restauração.

Restaurar dados de email do Microsoft Exchange

Cada vez que o CA ARCserve D2D executa um backup com êxito, também é criada uma imagem de instantâneo pontual de seu backup. Essa coleta de pontos de recuperação permite localizar e especificar exatamente qual imagem de backup deve ser restaurada. Para o Microsoft Exchange Server, é possível procurar estes pontos de recuperação para localizar os objetos individuais (caixas de correio, pastas da caixa de correio ou email) que deseja recuperar. Para executar uma restauração granular do Exchange, a conta deve ter as permissões necessárias. Para obter mais informações, consulte o tópico Permissões necessárias para a conta do Exchange.

Observação: para o Microsoft Exchange Server 2007 ou mais recente, o MAPI (Messaging API) é um pré-requisito para a restauração granular do Exchange. Se o MAPI não estiver instalado no Exchange, Server, as restaurações em nível granular da caixa de correio ou de email podem falhar. Para obter mais informações sobre a instalação do MAPI no Exchange Server, consulte o tópico Central de download da Microsoft.

Para restaurar dados de email do Microsoft Exchange

1. Efetue logon no aplicativo e clique em Nó na barra de navegação.

   Na tela Nó, expanda o grupo que contém o nó que deseja restaurar.

   Clique na caixa de seleção ao lado do nó que deseja restaurar e, em seguida, clique em Restaurar na barra de ferramentas.

2. Na caixa de diálogo Restaurar, clique em Restaurar emails do Exchange.

   A caixa de diálogo Restaurar emails do Exchange é aberta.

3. Especificar o local do backup. Você pode especificar um local ou procurar o local onde as suas imagens de backup estão armazenadas. Se necessário, forneça as credenciais de nome de usuário e senha para acessar esse local. É possível clicar no ícone de validação em forma de seta verde para confirmar o correto acesso ao local de origem.

   A exibição do calendário realçará (em verde) todas as datas do período exibido que contiverem os pontos de recuperação para essa origem de backup.

4. Selecione a data no calendário para a imagem de backup que deseja restaurar.

   Os bancos de dados da caixa de correio do Exchange correspondentes a essa data são exibidos juntamente com a hora do backup, o tipo de backup que foi executado e o nome do backup.

5. Selecione um banco de dados da caixa de correio do Exchange que deseja restaurar e clique em Avançar.

   Observação: uma mensagem de notificação será exibida perguntando se você deseja gerar um catálogo de restauração granular do Exchange no momento. Caso selecione Não gerar um catálogo agora, não será possível procurar ou selecionar um ponto de recuperação granular. Como resultado, só será possível executar a restauração completa do banco de dados por meio da caixa de diálogo Procurar pontos de recuperação para restaurar.

   A caixa de diálogo Opções de restauração é exibida e a lista correspondente do conteúdo da caixa de correio do banco de dados selecionado é relacionada.

   Observação: apenas a restauração de email é suportada. Restaurando o Calendário, Contatos, Notas e tarefas que não são suportados.

6. Selecione o nível de objetos do Exchange para restauração (caixa de correio, pasta ou email individual).

   Observação: é possível selecionar todo o conteúdo, parte do conteúdo ou vários objetos do Exchange para restauração.

   a. Se for selecionado um banco de dados de caixa de correio, todas as caixas de correio do banco de dados serão restauradas.

   b. Se for selecionado um nível de caixa de correio, todo o conteúdo correspondente (pastas e emails individuais) da caixa de correio será restaurado.

   c. Se for selecionado o nível de pasta de caixa de correio, todo o conteúdo de email correspondente da pasta será restaurado.

   d. Se for selecionado o nível de email individuais, apenas os objetos de email selecionados serão restaurados.

      Observação: apenas para o Exchange 2003, se o email individual tiver sido restaurado e enviado por meio de qualquer cliente de email diferente do Outlook e se, durante o backup, havia no email algum tipo de marcador de status de sinalizador anexado, o email será restaurado, mas o marcador anexado não será incluído nele.

7. Clique em Avançar.
8. Selecione o destino da restauração.

   As opções disponíveis são restaurar no local original do backup ou restaurar em um local diferente.

   Observações:

   - Ao restaurar uma caixa de correio ou email (no local original ou em um local alternativo), verifique se o destino está disponível, caso contrário, a tentativa de restauração falhará. O CA ARCserve D2D apenas valida o destino quando a tarefa de restauração é enviada.
   - Se tentar restaurar emails em um computador em que os endereços de email não são válidos (não existe no domínio) ou se o usuário não está registrado na caixa de correio, alguns campos podem não ser os mesmos ao fazer o backup.
   - Para o Exchange 2010, os itens arquivados da caixa de correio podem ser restaurados no local original. Os itens arquivados da caixa de correio só podem ser restaurados em um local diferente ou em um disco local. Além disso, os itens regulares da caixa de correio não podem ser restaurados em caixas de correio arquivadas.

   Restaurar no local original

   Restaura os emails no local original a partir do qual a imagem de backup foi capturada. Os emails manterão a mesma hierarquia e serão restaurados em sua pasta e caixa de correio originais.

   - Se o computador atual não for o servidor ativo do Exchange, o CA ARCserve D2D detectará o local do servidor ativo e restaurará os emails nesse servidor.
   - Se a caixa de correio tiver sido movida para outro servidor do Exchange, mas ainda estiver na mesma organização, o CA ARCserve D2D detectará o novo servidor do Exchange em que a caixa de correio original reside e fará a restauração nesse servidor.
   - Se o nome de exibição da caixa de correio tiver sido alterado, qualquer tentativa de restaurá-la (por meio de uma sessão de backup anterior) em seu local original falhará, pois o CA ARCserve D2D não conseguirá localizar o nome alterado. Para resolver o problema, é possível especificar a restauração da caixa de correio em um local alternativo.

Apenas arquivo de despejo

Restaura os emails em um disco. Este disco local deve ser um caminho local. Os emails restaurados manterão a mesma hierarquia que tinham na caixa de correio do Exchange correspondente. O nome do arquivo é o assunto do email.

Observação: se o assunto do email, nome da pasta ou nome da caixa de correio incluir os seguintes caracteres, o caractere será substituído por hífen (-) no nome do arquivo: \ / : * ? " < > |

Há duas opções para resolver uma situação de conflito em um sistema de arquivos. Dois arquivos no sistema de arquivos não podem existir na mesma pasta, ao passo que os emails do Exchange podem.

- **Renomear--**se houver um arquivo no disco com o mesmo nome que o assunto do email, o CA ARCserve D2D nomeará o assunto e acrescentará um número ao final do assunto.
- **Substituir -** se houver um arquivo no disco com o mesmo nome que o assunto do email, o CA ARCserve D2D substituirá o arquivo.

Restaurar em um local diferente

Restaura os emails em um local especificado ou permite procurar o local em que as imagens de backup serão restauradas. O destino deve ser uma caixa de correio na mesma organização do Exchange, e um novo nome da pasta é necessário. (Se estiver tentando restaurar emails em um local diferente, o destino não pode ser uma pasta pública.)

Após especificar o nome de usuário e a senha, clique no botão Procurar para navegar por uma lista de todos os servidores do Exchange, grupos de armazenamento, bancos de dados do Exchange e caixas de correio na organização atual.

Selecione a caixa de correio como o destino.

9. Clique em Avançar.

   A caixa de diálogo Resumo da restauração é exibida.

10. Examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.

    - Se as informações de resumo não estiverem corretas, clique em Anterior e volte à caixa de diálogo em questão para alterar a configuração incorreta.
    - Se as informações de resumo estiverem corretas, clique em Concluir para iniciar o processo de restauração.

    Observação: quando a tarefa de restauração e de geração de catálogo da Restauração granular do Exchange está em andamento, a sessão de backup está montada. Não executar nenhuma operação (formato, alterar letra de unidade, excluir partição, etc.) no volume montado.

Exibir Logs do Gerenciador do CA ARCserve Central Protection

O Log de exibição contém informações abrangentes sobre todas as operações executadas pelo aplicativo. O log fornece uma trilha de auditoria de todas as tarefas executadas (com as atividades mais recentes listadas primeiro) e pode ser útil para a solução dos problemas que podem ocorrer.

Para exibir logs do Gerenciador do CA ARCserve Central Protection

1. Na página inicial, clique em Exibir logs na barra de navegação.

   A tela Exibir logs é exibida.

2. Nas listas suspensas, especifique as informações de log que você deseja exibir.

   - **Gravidade:** permite especificar a gravidade do log que você deseja exibir. É possível especificar as seguintes opções de gravidade:

     - **Todos -** permite exibir todos os logs, independentemente da gravidade.
     - **Informações -** permite exibir apenas os logs que descrevem informações gerais.
     - **Erros -** permite exibir apenas os logs que descrevem erros graves que ocorreram.
     - **Avisos -** permite exibir apenas os logs que descrevem avisos de erros que ocorreram.
     - **Erros e avisos -** permite exibir apenas erros graves e aviso de erros que ocorreram.

- **Módulo -** permite especificar o módulo para o qual você deseja exibir logs. É possível especificar as seguintes opções de módulo:
  - **Todos -** permite exibir logs sobre todos os componentes do aplicativo.
  - **Comum -** permite exibir logs sobre processos comuns.
  - **Importar nós a partir da detecção** - permite exibir logs em nós que foram importados somente a partir da detecção.
  - **Importar nós do HyperVisor** -- Permite exibir logs em nós que foram importados somente do Hypervisor.
  - **Importar nós do arquivo--** permite exibir apenas os logs sobre o processo de importação de nós no aplicativo de um arquivo.
  - **Gerenciamento de diretivas -** permite exibir apenas os logs sobre gerenciamento de diretivas.
  - **Sincronização do CA ARCserve Backup** - permite exibir apenas os logs sobre a sincronização de dados do CA ARCserve Backup.
  - **Sincronização do CA ARCserve D2D** - permite exibir apenas os logs sobre a sincronização de dados do CA ARCserve D2D.
  - **Atualizações do CA ARCserve D2D** - permite exibir apenas os logs sobre as alterações feitas no CA ARCserve D2D.
  - **Atualizações** - permite exibir apenas os logs sobre a atualização do aplicativo.
  - **Enviar tarefas de backup do CA ARCserve D2D** - permite exibir apenas os logs sobre tarefas de backup do CA ARCserve D2D enviadas.
  - **Verificação prévia** - permite exibir apenas os logs sobre as operações de verificação prévia.
  - **Enviar tarefas de backup da VM** - permite exibir apenas os logs sobre tarefas de backup da máquina virtual enviadas.
- **Nome do nó -** permite exibir apenas os logs de um nó específico.

  Observação: esse campo suporta os caracteres curinga '*' e '?'. Por exemplo, digite 'lod*' para retornar todos os logs de atividades para o nome de computador iniciado por 'lod'.

Observação: as opções de Gravidade, Módulo e Nome do nó podem ser aplicadas em grupo. Por exemplo, você pode exibir erros (Gravidade) que estão relacionados a atualizações (Módulo) para o nó X (Nome do nó).

Clique em Atualizar.

Os logs são exibidos com base nas opções de exibição especificadas.

Observação: a hora exibida no log tem como base o fuso horário em que o servidor do Gerenciador do CA ARCserve Central Protection reside.

Adicionar links à barra de navegação

Cada CA ARCserve Central Applications possui um link Adicionar nova guia na barra de navegação. Use este recurso para adicionar entradas na barra de navegação para outros aplicativos da web que deseja gerenciar. No entanto, para cada aplicativo instalado, um novo link é automaticamente adicionado à barra de navegação. Por exemplo, se você tiver instalado o CA ARCserve Central Reporting e o CA ARCserve Central Virtual Standby no "computador A" e, em seguida, iniciar o CA ARCserve Central Reporting, o CA ARCserve Central Virtual Standby é automaticamente adicionado à barra de navegação.

Observação: cada aplicativo instalado é detectado somente se outros CA ARCserve Central Applications estiverem no mesmo computador.

Siga estas etapas:

1. Na barra de navegação do aplicativo, clique no link Adicionar nova guia.
2. Especifique o nome e o URL do aplicativo ou site que deseja adicionar. Por exemplo, www.google.com.

   Como opção, é possível especificar o local de um ícone.
3. Clique em OK.

   A nova guia é adicionada à parte inferior da barra de navegação.

Lembre-se das seguintes considerações:

- Para sua conveniência, o link do Suporte da CA é adicionado por padrão.

É possível remover a nova guia, destacando a guia e clicando no link Remover.

Aplicando práticas recomendadas

Considere as práticas recomendadas a seguir para o aplicativo <egcm >:

- O CA ARCserve Central Applications pode recuperar dados de um nó específico a partir de um computador remoto por meio de comunicações entre o computador local e o computador remoto do CA ARCserve Central Applications.

  Para garantir que o acesso remoto opere com êxito, as seguintes restrições são necessárias:

  - **Restrição de rede--** o compartilhamento do administrador remoto chamado 'admin$' no computador remoto deve estar ativado.
  - **Restrição da conta de usuário--**para efetuar logon no CA ARCserve Central Applications, use a conta do administrador de boletins do computador local do CA ARCserve Central Applications ou adicione privilégios administrativos ao computador local e remoto do CA ARCserve Central Applications.

  Observação: para adicionar um nó, é necessário ter privilégios administrativos no computador remoto.

- Para adicionar nós usando o nome do nó ou endereço IP em um computador Windows Server 2008 R2, use a conta com base em um dos seguintes requisitos:

  - Se estiver usando a conta Grupo de administradores a partir do computador do CA ARCserve Central Applications e do computador remoto para efetuar logon no CA ARCserve Central Applications, é possível usar a mesma conta para adicionar um nó.
  - Se você usar a conta Administrador de boletins do computador do CA ARCserve Central Applications para efetuar logon no CA ARCserve Central Applications, use a conta Grupo de administradores a partir do computador remoto para adicionar um nó.

- Para detectar nós no Active Directory, execute uma das opções a seguir:

  - Se instalar o CA ARCserve Central Applications em um nó conectado a um domínio do Windows, o CA ARCserve Central Applications poderá ter acesso às informações do Active Directory que reside no controlador de domínio.
  - Se instalar o CA ARCserve Central Applications em um nó que esteja conectado a um grupo de trabalho, é necessário que você execute a seguinte linha de comando em uma janela de comando para confirmar que o CA ARCserve Central Applications tem acesso ao controlador de domínio associado:

    ```
    nltest /dsgetdc:%domain_name%
    ```

    Observação: se esta opção falhar com um status de ERROR_NO_SUCH_DOMAIN (1355), será necessário ajustar as configurações de rede.

Alterar o protocolo de comunicação do servidor

Por padrão, o CA ARCserve Central Applications usa o protocolo HTTP (Hypertext Transfer Protocol) para comunicação entre todos os seus componentes. Caso esteja preocupado com a segurança das senhas comunicadas entre esses componentes, é possível alterar o protocolo em uso para HTTPS (Hypertext Transfer Protocol Secure). Além disso, se você não precisar deste nível extra de segurança, é possível alterar o protocolo em uso para HTTP.

Siga estas etapas:

1. Efetue logon no computador no qual o aplicativo está instalado usando uma conta administrativa ou uma conta com privilégios administrativos.

   Observação: se não efetuar logon usando uma conta administrativa ou uma conta com privilégios administrativos, configure a linha de comando para ser executada usando o privilégio Run as Administrator.

2. Abra a linha de comando do Windows.

3. Siga um destes procedimentos:

   - **Para alterar o protocolo de HTTP para HTTPS:**

     Inicie a ferramenta de utilitário changeToHttps.bat no seguinte local padrão (o local da pasta BIN pode variar dependendo de onde você instalou o aplicativo):

     `C:\Arquivos de Programas\CA\ARCserve Central Applications\BIN`

     Quando o protocolo for alterado com êxito, a seguinte mensagem será exibida:

     `O protocolo de comunicação foi alterado para HTTPS.`

   - **Para alterar o protocolo de HTTPS para HTTP:**

     Inicie a ferramenta de utilitário changeToHttp.bat no seguinte local padrão (o local da pasta BIN pode variar dependendo de onde você instalou o aplicativo):

     `C:\Arquivos de Programas\CA\ARCserve Central Applications\BIN`

     Quando o protocolo for alterado com êxito, a seguinte mensagem será exibida:

     `O protocolo de comunicação foi alterado para HTTP.`

4. Reinicie o navegador e reconecte-se ao CA ARCserve Central Applications.

   Observação: quando você altera o protocolo para HTTPS, um aviso é exibido no navegador web. Esse comportamento ocorre devido a um certificado de segurança autoassinado que solicita que você ignore o aviso e continue ou adicione esse certificado ao navegador para evitar que o aviso seja exibido novamente.

Capítulo 5: Integração do Gerenciador do CA ARCserve Central Protection às ferramentas do servidor de gerenciamento de TI

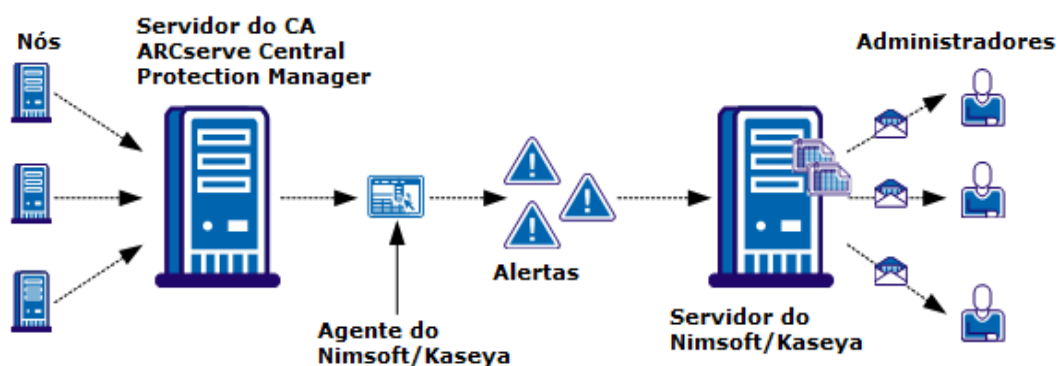
Esta seção contém os seguintes tópicos:

Como o Gerenciador do CA ARCserve Central Protection se integra ao Nimsoft e ao Kaseya

É possível configurar o Gerenciador do CA ARCserve Central Protection para publicar informações sobre mensagens de alerta em tempo real para as ferramentas de gerenciamento de infraestrutura do servidor de gerenciamento de TI. Esse recurso permite que os administradores de gerenciamento de TI de servidores responda aos alertas do Gerenciador do CA ARCserve Central Protection de modo eficaz.

O Gerenciador do CA ARCserve Central Protection integra-se às ferramentas de gerenciamento de infraestrutura do servidor de gerenciamento de TI:

- Nimsoft
  - Servidor: 5.11
  - Robô: 5.32
  - Unified Monitoring Portal: 2.1.2
- Kaseya
  - Servidor: 6.1.0.0
  - Agente: 6.1.0.6

O diagrama a seguir ilustra como o Gerenciador do CA ARCserve Central Protection se integra ao Nimsoft e ao Kaseya:

O servidor do Gerenciador do CA ARCserve Central Protection monitora os nós onde o CA ARCserve D2D está instalado. Quando o servidor do Gerenciador do CA ARCserve Central Protection detecta uma condição do alerta, ele envia os alertas ao agente do Nimsoft ou do Kaseya que está instalado no servidor do Gerenciador do CA ARCserve Central Protection. O agente enviará os alertas ao servidor do Nimsoft ou do Kaseya imediatamente.

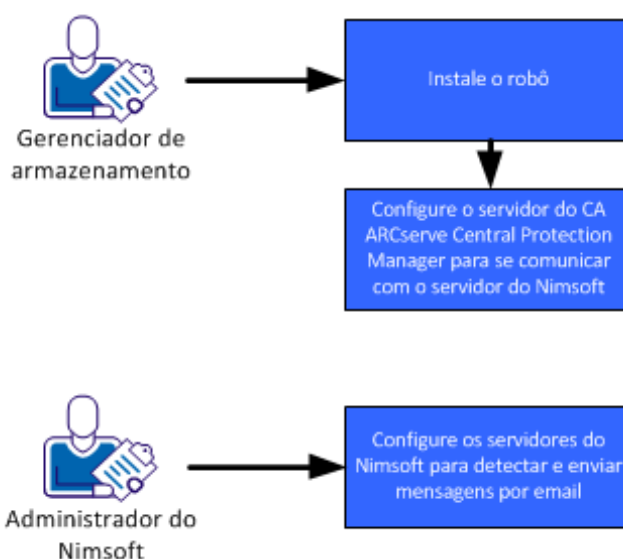
O Gerenciador do CA ARCserve Central Protection monitora os alertas que se originam dos seguintes aplicativos:

- CA ARCserve D2D
- CA ARCserve Central Virtual Standby
- CA ARCserve Central Host-Based VM Backup
- Gerenciador do CA ARCserve Central Protection

O servidor do Nimsoft ou Kaseya gera relatórios sobre os nós que executam os aplicativos que os administradores podem exibir usando as ferramentas de gerenciamento do Nimsoft e do Kaseya. Os servidores do Nimsoft e do Kaseya podem ser configurados para enviar mensagens de email aos administradores com base nos critérios predefinidos.

Como integrar o Gerenciador do CA ARCserve Central Protection ao Nimsoft

Os gerenciadores de armazenamento podem configurar o Gerenciador do CA ARCserve Central Protection para comunicar as mensagens de alerta aos servidores do Nimsoft. Os administradores do Nimsoft podem configurar as ferramentas de gerenciamento de infraestrutura de TI para detectar alertas do Gerenciador do CA ARCserve Central Protection, gerar relatórios de alerta e enviar mensagens de email. Os administradores podem usar os relatórios para gerenciar a integridade dos nós do CA ARCserve D2D.

O diagrama a seguir ilustra como os gerenciadores de armazenamento integram o Gerenciador do CA ARCserve Central Protection às ferramentas de gerenciamento de infraestrutura de TI do Nimsoft:

Siga estas etapas para integrar o Gerenciador do CA ARCserve Central Protection ao Nimsoft:

1. Instale o robô (na página 164).
2. Configure o servidor do Gerenciador do CA ARCserve Central Protection para se comunicar com o servidor do Nimsoft (na página 165).
3. Configure os servidores do Nimsoft para detectar e enviar emails (na página 166).

Observação: quando os servidores do Gerenciador do CA ARCserve Central Protection enviam mensagens de alerta que contenham caracteres localizados aos servidores do Nimsoft, estes caracteres podem ser exibidos como texto ilegível no console de alarmes do Nimsoft Unified Monitoring Portal. Para ajudar a evitar que este comportamento ocorra, configure o servidor do Nimsoft para usar a codificação UTF-8. Para obter mais informações, consulte a seção Caracteres de servidores localizados são exibidos como texto ilegível no console de alarmes do Nimsoft UMP, no Guia do Usuário do Gerenciador do CA ARCserve Central Protection.

Instale o robô

É necessário instalar o robô no servidor do Gerenciador do CA ARCserve Central Protection. O robô permite que o Gerenciador do CA ARCserve Central Protection se comunique com o servidor e envie mensagens de alerta em tempo real para servidores do Nimsoft.

Observação: antes de executar o programa de instalação, verifique se você possui uma licença válida.

Siga estas etapas:

1. Faça download ou copie o arquivo de instalação do robô para o computador.

   Clique duas vezes em *NimBUS Robot.exe* para iniciar a instalação.

   A caixa de diálogo do Contrato de licença será exibida.

2. Clique em Sim na caixa de diálogo de licença para iniciar a instalação.

   A caixa de diálogo Choose Destination Location é exibida.

3. Especifique o local onde deseja instalar o robô ou clique em Avançar para aceitar o diretório padrão.

   A caixa de diálogo Choose Setup Type é aberta.

4. Clique em Instalação normal e em Avançar.

   A caixa de diálogo Nimsoft Domain é aberta para exibir uma lista de domínios detectados.

5. Clique na caixa de seleção ao lado da opção Choose to connect to the network interface through IP address e, em seguida, clique em Avançar.

   A caixa de diálogo Specify Nimsoft Hub IP Address é exibida.

6. No campo Hub IP, especifique o endereço IP do hub do Nimsoft para onde deseja que o servidor do Gerenciador do CA ARCserve Central Protection envie as mensagens de alerta.

   Clique em Avançar.

   A caixa de diálogo Opções é aberta.

7. Preencha os seguintes campos da caixa de diálogo Opções:

   (Opcional) a primeira porta do probe

   Permite especificar o número da primeira porta a ser usada ao iniciar os probes.

   Observação: não especifique uma porta para permitir que o sistema operacional gere portas aleatórias.

   Modo passivo

   Especifique esse modo quando o robô não puder se comunicar com o hub do Nimsoft. Se o hub do Nimsoft puder comunicar com o servidor do Gerenciador do CA ARCserve Central Protection, clique na caixa de seleção ao lado do modo passivo.

   Observação: com esta opção especificada, adicione o robô passivo à configuração do hub manualmente.

   Clique em Avançar.

   A caixa de diálogo Iniciar a cópia de arquivos é exibida.

8. Clique em Avançar.

   O programa de instalação instala o robô.

9. Quando a instalação terminar, clique em Concluir.

O robô foi instalado.

Configure os servidores do Gerenciador do CA ARCserve Central Protection para se comunicar com os servidores do Nimsoft

O Gerenciador do CA ARCserve Central Protection permite enviar mensagens de alerta aos servidores de gerenciamento de TI do Nimsoft. Para enviar as informações de alerta, configure o servidor do Gerenciador do CA ARCserve Central Protection para se comunicar com o servidor do Nimsoft.

Siga estas etapas:

1. Efetue logon no Gerenciador do CA ARCserve Central Protection e clique em Configuração na barra de navegação.

   A opção Configuração é exibida.

2. Clique em Configuração do servidor de gerenciamento de TI na lista Configuração.

   As opções de configuração do servidor de gerenciamento de TI são exibidas.

3. Proceda da seguinte maneira:
   a. Clique em Ativar.
   b. Clique em Nimsoft.
   c. Especifique um método de repetição. O método de repetição define os dias da semana para o reenvio das notificações de alerta para o servidor do Nimsoft quando o processo de envio original falhar. O processo de envio de alertas pode falhar quando o servidor do Nimsoft estiver offline ou indisponível.
   d. Especifique um cronograma. O cronograma define a hora do dia para enviar novamente as notificações de alerta para o servidor do Nimsoft.

   Clique em Salvar.

O servidor do Gerenciador do CA ARCserve Central Protection é configurado para se comunicar com o servidor do Nimsoft.

Configure o servidor do Nimsoft para detectar e enviar mensagens de email

Os administradores do Nimsoft podem configurar o subconsole de alarmes para enviar mensagens de email para destinatários designados ao detectar mensagens de alerta dos servidores do Gerenciador do CA ARCserve Central Protection. Para obter mais informações, consulte a documentação do Nimsoft.

Exibir informações sobre alertas no subconsole de alarmes do Nimsoft

O subconsole de alarmes do Nimsoft permite que os administradores exibam informações sobre alertas do Gerenciador do CA ARCserve Central Protection. O subconsole de alarmes do Nimsoft fornece as seguintes informações sobre os alertas do Gerenciador do CA ARCserve Central Protection:

Nome do host

Especifica o nome de host do servidor do Gerenciador do CA ARCserve Central Protection que envia o alerta para o servidor do Nimsoft.

Origem

Especifica o endereço IP do servidor do Gerenciador do CA ARCserve Central Protection que envia o alerta para o servidor do Nimsoft.

Gravidade

Especifica a gravidade do alerta enviado ao servidor do Nimsoft.

Subsistema

Especifica o nome do host do servidor que encontrou a condição de alerta.

Exemplo: a condição do alerta ocorreu em um servidor do CA ARCserve D2D. O campo do sistema especifica o nome do host do servidor do CA ARCserve D2D.

ID do subsistema

Especifica o endereço IP do servidor que encontrou a condição de alerta.

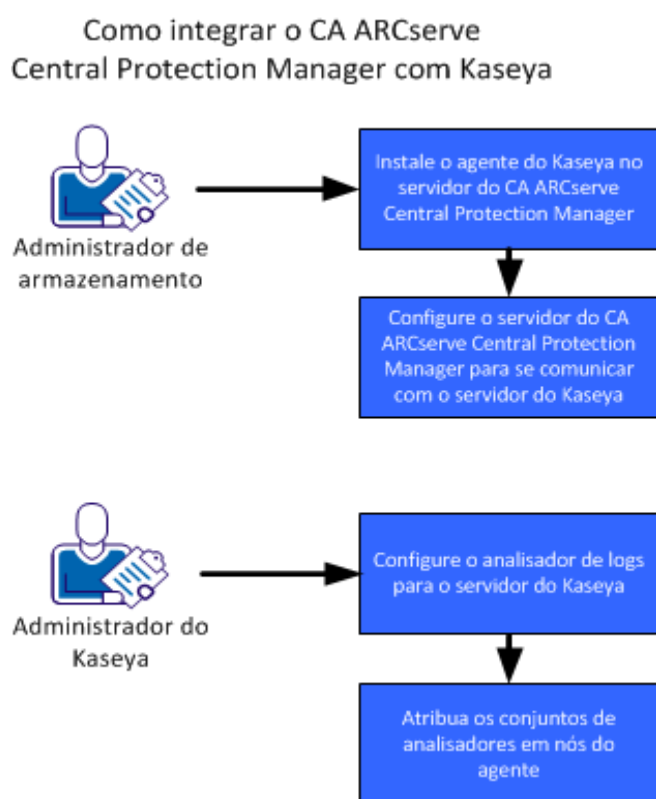
O subconsole de alarmes permite que os administradores do Nimsoft executem várias tarefas, como as seguintes:

- Configurar o subconsole de alarmes para enviar mensagens de email para destinatários designados ao detectar alertas
- Exibir o histórico de alertas
- Confirmar alertas
- Atribuir alertas para técnicos

Observação: para obter mais informações sobre como usar o subconsole de alarmes do Nimsoft, consulte a documentação do Nimsoft.

Como integrar o Gerenciador do CA ARCserve Central Protection ao Kaseya

Os gerenciadores de armazenamento podem configurar o Gerenciador do CA ARCserve Central Protection para comunicar as mensagens de alerta aos servidores do Kaseya. Os administradores do Kaseya podem configurar as ferramentas de gerenciamento de infraestrutura de TI do Kaseya para detectar alertas do Gerenciador do CA ARCserve Central Protection, gerar relatórios de alerta e enviar emails. Os administradores podem usar os relatórios para gerenciar a integridade dos nós do CA ARCserve D2D.

O diagrama a seguir ilustra como os gerenciadores de armazenamento integram o Gerenciador do CA ARCserve Central Protection à ferramenta de gerenciamento de infraestrutura de TI do Kaseya:

Siga estas etapas para integrar o Gerenciador do CA ARCserve Central Protection ao kaseya:

1. Instale o agente do Kaseya no servidor do Gerenciador do CA ARCserve Central Protection (na página 169).
2. Configure o servidor do Gerenciador do CA ARCserve Central Protection para se comunicar com o servidor do Kaseya (na página 170).

3. Configure o analisador de log do servidor do Kaseya (na página 170).
4. Atribua os conjuntos de analisador aos nós do agente (na página 173).

Instale o agente do Kaseya

Instale o agente do Kaseya no Gerenciador do CA ARCserve Central Protection para permitir a comunicação com o servidor do Kaseya. Instale o agente implantando-o a partir do console de gerenciamento de TI do Kaseya.

Siga estas etapas:

1. Abra uma janela do navegador e efetue logon no console de gerenciamento de TI do Kaseya.

   Na barra de navegação no lado esquerdo da janela, clique em Agente.

   As opções de agente são exibidas.

2. Expanda os agentes da instalação e clique em Implantar agentes.

   As opções de implantação de agentes são exibidas.

3. Clique em uma das seguintes opções:

   Clicar para fazer download do agente padrão

   Permite fazer download e salvar o arquivo de instalação no computador de destino.

   Após a conclusão do download, execute o arquivo de instalação do agente diretamente no computador de destino.

   Criar pacote

   Permite criar um utilitário de instalação de pacotes para instalar o agente em um ou mais computadores. Siga as instruções na tela para criar o pacote de instalação. Para obter mais informações, consulte a documentação do Kaseya.

O agente está instalado.

Configure o servidor do Gerenciador do CA ARCserve Central Protection para se comunicar com o servidor do Kaseya.

O Gerenciador do CA ARCserve Central Protection permite enviar mensagens de alerta aos servidores de gerenciamento de TI do Kaseya. Para enviar as informações de alerta, configure o servidor do Gerenciador do CA ARCserve Central Protection para se comunicar com o servidor do Kaseya.

Siga estas etapas:

1. Efetue logon no Gerenciador do CA ARCserve Central Protection e clique em Configuração na barra de navegação.

   A opção Configuração é exibida.

2. Clique em Configuração do servidor de gerenciamento de TI, na lista Configuração.

   As opções de configuração do servidor de gerenciamento de TI são exibidas.

3. Proceda da seguinte maneira:

   a. Clique em Ativar.

   b. Clique em Kaseya.

   c. Especifique um método de repetição. O método de repetição define os dias da semana para o reenvio das notificações de alerta para o servidor do Kaseya quando o processo de envio original falhar. O processo de envio de alertas pode falhar quando o servidor do Kaseya estiver offline ou indisponível.

   d. Especifique um cronograma. O cronograma define a hora do dia para enviar novamente as notificações de alerta para o servidor do Kaseya.

   Clique em Salvar.

O servidor do Gerenciador do CA ARCserve Central Protection é configurado para se comunicar com o servidor do Kaseya.

Configure o analisador de log do servidor do Kaseya.

Para exibir informações sobre os alertas do Gerenciador do CA ARCserve Central Protection, configure o servidor do Kaseya para ler os dados nos arquivos de log de alertas do Gerenciador do CA ARCserve Central Protection.

Siga estas etapas:

1. Abra uma janela do navegador e efetue logon no console de gerenciamento de TI do Kaseya.

2. Na barra de navegação no lado esquerdo da janela, clique em Monitor.

   As opções de monitor são exibidas.

3. Expanda o monitoramento de log e clique em Analisador de log.

   As opções de configuração do analisador de log são exibidas.

4. Na lista Machine.Group ID, clique na caixa de seleção próxima ao servidor do Gerenciador do CA ARCserve Central Protection.

   Na caixa de listagem suspensa Log File Parser, clique em <Select Log Parser>.

   Clique em Novo.

   A caixa de diálogo Log File Parser Definition é aberta.

5. Preencha os seguintes campos na caixa de diálogo Log File Parser Definition:

   Nome do analisador

   Define o nome do arquivo de analisador de arquivos de log.

   Caminho do arquivo de log

   Define o caminho do arquivo de log no servidor do Gerenciador do CA ARCserve Central Protection. O caminho para o arquivo de log é:

   ```
   <HOME_CA ARCserve Central Applications>\ITMgmtIntegration\<log_fle_name>
   ```

   O Gerenciador do CA ARCserve Central Protection gera os arquivos de log que oferecem suporte a caracteres Unicode e não-Unicode. Os nomes do arquivo de log são os seguintes:

   Não-Unicode:

   ```
   CentralAppAlertsForKaseyaANSI.log
   ```

   Unicode:

   ```
   CentralAppAlertsForKaseyaUTF8.log
   ```

   Importante: O console de gerenciamento de TI do Kaseya não oferece suporte a caracteres Unicode. Portanto, use o arquivo de log denominado CentralAppAlertsForKaseyaANSI.log.

   Caminho de arquivamento de log

   Define o caminho do arquivo de log arquivado no servidor do Gerenciador do CA ARCserve Central Protection. Por padrão, o Protection Manager arquiva o arquivo de log quando ele excede 10 MB.

   Observação: para especificar um outro valor quando o Protection Manager arquiva o arquivo de log, altere o valor de MaxLogFileSize (em MB) no seguinte arquivo:

   ```
   <HOME_CA ARCserve Central
   Applications>\ITMgmtIntegration\Configuration\Edge-ITMgmtIntegration.INI
   ```

   Descrição

   Define a descrição do arquivo do analisador de arquivos de log.

Modelo

Define o formato dos dados contidos no arquivo de log no servidor do Gerenciador do CA ARCserve Central Protection. Use a seguinte sintaxe:

```
$CACentral Protection Manager Machine Name$ [$Alert Generated Product$]
$Alert Generated Machine Name$ $Severity$ $Send Time From Origin Product$
$Alert Message$
```

Modelo de saída

Define o formato dos dados de saída no servidor do Kaseya. Use a seguinte sintaxe:

```
$Protection Manager Server$ $Generated by$ $Host Name$ $Severity$ $Sent$
$Message$
```

Parâmetros do arquivo de log

Crie os seguintes parâmetros do arquivo de log:

Observação: especifique o tipo (de parâmetro) para salvar o parâmetro e clique em Aplicar.

Nome da máquina do CA ARCserve Central Protection Manager

Tipo: sequência de caracteres

Produto de alerta gerado

Tipo: sequência de caracteres

Nome da máquina que gerou o alerta

Tipo: sequência de caracteres

Gravidade

Tipo: sequência de caracteres

Tempo de envio do produto de origem

Tipo: DateTime

Formato: DD-MM-AAAA hh:mm:ss

Mensagem de alerta

Tipo: sequência de caracteres

Clique em Salvar.

A definição do analisador de log é salva.

6. Clique em Fechar.

A caixa de diálogo Log Parser Definition é fechada e o arquivo de definição do analisador de log é criado e aplicado ao servidor do Gerenciador do CA ARCserve Central Protection.

Atribuir os conjuntos do analisador no servidor do Kaseya

Configure os conjuntos de analisadores para filtrar informações sobre alertas do Gerenciador do CA ARCserve Central Protection no console de gerenciamento do Kaseya. Os conjuntos de analisadores definem as condições filtradas. Por exemplo, é possível filtrar os alertas com base no nível de gravidade, falhas de backup, e assim por diante.

Siga estas etapas:

1. Abra uma janela do navegador e efetue logon no console de gerenciamento de TI do Kaseya.
2. Na barra de navegação no lado esquerdo da janela, clique em Monitor.

   As opções de monitor são exibidas.
3. Expanda o monitoramento de log e clique em Assign Log Parser.

   As opções de conjuntos de analisadores de log de atribuição são exibidas.
4. Na seção Atribuir conjuntos de analisadores de log para computadores selecionados, especifique as opções de alertas necessárias.
5. Na lista suspensa Selecionar o analisador de logs, clique no analisador de logs ao qual deseja atribuir os conjuntos de analisadores.

   Na lista suspensa Define parser sets, clique em <New Parser Set>.

   A caixa de diálogo Edit Parser Set é aberta.
6. No campo Nome do conjunto de analisadores, especifique um nome para o conjunto de analisadores e clique em Novo.

   As opções de análise são exibidas.
7. Especifique os valores a seguir:

   Coluna do analisador

   Define o parâmetro que deseja filtrar.

   Operador

   Define como deseja filtrar os dados contidos no parâmetro.

   Arquivo de parâmetro

   Define o valor do parâmetro que deseja filtrar.

   Clique em Adicionar e em Fechar.

   O filtro é aplicado ao conjunto de analisadores e a caixa de diálogo Edit Parser Set é fechada.

   Observação: para ver exemplos de como especificar filtros de conjunto de analisadores, consulte o tópico Exemplos de filtros de conjunto de analisadores.

8. Na lista suspensa Selecionar o analisador de logs, clique no analisador de logs que deseja aplicar.

   Na lista suspensa Definir conjuntos de analisadores, clique no conjunto de analisador criado.

   Na coluna IDs da máquina, clique na caixa de seleção ao lado dos servidores que deseja aplicar o conjunto de analisadores.

   Clique em Aplicar.

O analisador de logs e o conjunto de analisadores são atribuídos.

Exemplos de filtros de conjunto de analisadores

Para criar conjuntos de analisadores que filtram somente os alertas que contêm erros, especifique os seguintes valores:

Coluna do analisador

Gravidade

Operador

Igual a

Filtro de parâmetro

erro

Para criar conjuntos de analisadores que exibem todos os alertas, independentemente do nível de gravidade, especifique os seguintes valores:

Coluna do analisador

Gravidade

Operador

Contém

Filtro de parâmetro

erro, aviso, informação

Para criar conjuntos de analisadores que exibem somente os alertas de backups com falha, especifique os seguintes valores:

Coluna do analisador

Mensagem de alerta

Operador

Contém

Filtro de parâmetro

backup, falha

Configure os servidores do Kaseya para detectar e enviar mensagens de email.

Os administradores do Kaseya podem configurar o subconsole de alarmes para enviar mensagens de email para destinatários designados ao detectar mensagens de alerta dos servidores do Gerenciador do CA ARCserve Central Protection. Para obter mais informações, consulte a documentação do Kaseya.

Exibir informações sobre alertas no monitor do log de agente do Kaseya

O monitor do log de agente do Kaseya permite exibir logs de alerta de acordo com os critérios definidos no analisador de logs e no conjunto de analisadores. Os logs permitem identificar e realizar ações corretivas para corrigir a condição do alerta.

Para exibir informações sobre alertas no monitor do log de agente do Kaseya

1. Abra uma janela do navegador e efetue logon no console de gerenciamento de TI do Kaseya.

   Na barra de navegação no lado esquerdo da janela, clique em Agente.

   As opções de agente são exibidas.

2. Expanda o status da máquina e clique em Logs do agente.

   Os logs do agente são exibidos no lado direito da janela.

3. Na lista de servidores, clique no servidor ao qual deseja exibir informações.

   Clique em Atualizar.

As informações sobre as mensagens de alerta são exibidas para o servidor especificado.

Capítulo 6: Solução de problemas do Gerenciador do CA ARCserve Central Protection

Esta seção fornece informações sobre solução de problemas para ajudá-lo a identificar e resolver problemas que possam ocorrer durante o uso do Gerenciador do CA ARCserve Central Protection.

Esta seção contém os seguintes tópicos:

Mensagens do tipo "Não é possível estabelecer conexão com o servidor especificado" são exibidas ao tentar adicionar nós

Válido em plataformas Windows.

Sintoma:

A mensagem a seguir é exibida quando se tenta adicionar ou estabelecer conexão com os nós da tela Nó.

```
Não é possível se conectar ao servidor especificado.
```

Solução:

Se a mensagem acima for exibida ao tentar adicionar nós a partir da tela Nó, as seguintes ações corretivas ajudam a resolver o problema:

- Verifique se o serviço do Windows Server está em execução na máquina virtual de origem (nó) e no servidor do Gerenciador do CA ARCserve Central Protection.
- Verifique se uma exceção do Windows Firewall foi aplicada ao serviço de compartilhamento de arquivo e impressora do Windows na máquina virtual de origem (nó) e no servidor do Gerenciador do CA ARCserve Central Protection.
- Verifique se uma exceção do Windows Firewall foi aplicada ao serviço Netlogon do Windows apenas se o nó não for integrante de um domínio. Execute esta tarefa na máquina virtual de origem (nó) e no servidor do Gerenciador do CA ARCserve Central Protection.
- Verifique se o valor aplicado ao modelo de compartilhamento e segurança para contas locais é Clássico. Para aplicar o valor Clássico proceda da seguinte maneira:

  Observação: execute as etapas a seguir na máquina virtual de origem (nó) e no servidor do Gerenciador do CA ARCserve Central Protection.

  1. Efetue logon no servidor do Gerenciador do CA ARCserve Central Protection e abra o Control Panel.
  2. No Painel de controle, abra Administrative Tools.
  3. Clique duas vezes em Diretiva de segurança local.

     A janela Diretiva de segurança local é exibida.

4. Nesta janela, expanda Diretivas locais e expanda Opções de segurança.

   As diretivas de segurança são exibidas.

5. Clique com o botão direito do mouse em Network access: Sharing and security model for local accounts e clique em Propriedades no menu pop-up.

   A caixa de diálogo Network access: Sharing and security model for local accounts properties é exibida.

6. Clique em Configuração de segurança local.

   Na lista suspensa, selecione Clássico - os usuários locais são autenticados como eles mesmos.

   Clique em OK.

- Verifique se o valor aplicado às Diretivas locais para o nível de autenticação do LAN Manager é definido para enviar LM & NTLMv2 - usar a segurança da sessão NTLMv2, se negociado. Para aplicar o valor, proceda da seguinte maneira:

  1. Efetue logon no servidor do Gerenciador do CA ARCserve Central Protection e abra o prompt de comando.

     Execute o seguinte comando

     ```
     secpol.msc
     ```

     A caixa de diálogo Configurações locais de segurança é exibida.

  2. Selecione as diretivas locais e clique em opções de segurança.

     Pesquise a segurança de rede: nível de autenticação do LAN Manager.

     Clique duas vezes na opção.

     A caixa de diálogo Propriedades é aberta

  3. Selecione a opção a seguir e clique em OK.

     ```
     enviar LM & NTLMv2 - usar a segurança da sessão NTLMv2, se negociado
     ```

  4. No prompt de comando, execute o seguinte:

     ```
     gpupdate
     ```

  O valor é aplicado.

Páginas da web em branco são exibidas ou ocorrem erros no Javascript

Válido para os sistemas operacionais Windows Server 2008 e Windows Server 2003.

Sintoma:

Ao abrir os sites da web do CA ARCserve Central Applications usando o Internet Explorer, páginas da web em branco são exibidas ou ocorrem erros no Javascript. O problema ocorre ao abrir o Internet Explorer em sistemas operacionais Windows Server 2008 e Windows Server 2003.

Esse problema ocorre nas seguintes condições:

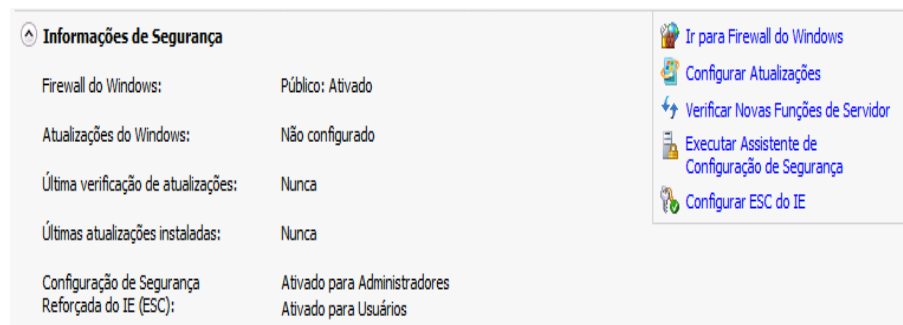
- Você está usando o Internet Explorer 8 ou Internet Explorer 9 para exibir o aplicativo e o navegador não reconhece o URL como um site confiável.
- Você está usando o Internet Explorer 9 para exibir o aplicativo e o protocolo de comunicação em uso é HTTPS.

Solução:

Para corrigir este problema, desative a opção Segurança aprimorada do Internet Explorer nos computadores usados para exibir o aplicativo.

Para desativar esta opção em sistemas Windows Server 2008, faça o seguinte:

1. Faça logon no computador com Windows Server 2008 que você usa para exibir os relatórios usando a conta de administrador ou uma conta que tenha privilégios administrativos.
2. Clique com o botão direito do mouse em Computador na área de trabalho e clique em Gerenciar para abrir a janela Gerenciador do servidor.
3. Na janela Gerenciador do servidor, clique em Gerenciador do servidor (nome do servidor).

   Na seção Server Summary, abra Security Information e clique em Configure IE ESC, conforme ilustrado abaixo:

   A caixa de diálogo Enhanced Security Configuration do Internet Explorer é aberta.

4. Neste caixa de diálogo, faça o seguinte:
   - Administrators--Click Desativado
   - Usuários--Clique em Desativar.

   Clique em OK.

A caixa de diálogo Internet Explorer Enhanced Security Configuration é fechada e segurança reforçada do Internet Explorer é desativada.

Para desativar esta opção em sistemas Windows Server 2003, faça o seguinte:

1. Faça logon no computador com Windows Server 2003 que você usa para exibir os relatórios usando a conta de administrador ou uma conta que tenha privilégios administrativos.
2. Abra o Painel de Controle do Windows e, em seguida, abra Add or Remove Programs.
3. Na caixa de diálogo Add or Remove Programs, clique na opção Add/Remove Windows Components para acessar a tela Windows Components Wizard.

   Desmarque a caixa de seleção próxima a Configuração de segurança aprimorada do Internet Explorer.

   Clique em Avançar.

   Siga as instruções na tela para concluir a instalação e clique em Concluir.

A opção Internet Explorer Enhanced Security é desativada.

As páginas da web não são carregadas corretamente ao efetuar logon nos nós do CA ARCserve D2D

Válido em plataformas Windows.

Sintoma:

As páginas da web em janelas do navegador não são carregadas corretamente, exibem mensagens de erro, ou ambos, ao efetuar logon em nós do CA ARCserve D2D na tela Nós.

Solução:

Esse comportamento afeta principalmente os navegadores Internet Explorer. As páginas da web podem não ser carregadas corretamente quando scripts ativos, controles ActiveX ou programas Java estiverem desativados no computador ou bloqueados na rede.

É possível corrigir o problema com a atualização da janela do navegador. No entanto, se a atualização do navegador não corrigir o problema, faça o seguinte:

1. Abra o Internet Explorer.

   No menu Ferramentas, clique em Opções da Internet.

   A caixa de diálogo Opções da Internet é aberta.

2. Clique na guia Segurança.

   As opções de segurança são exibidas:

3. Clique em Zona da Internet.

   As opções de zona da Internet são exibidas.

4. Clique em Nível personalizado.

   A caixa de diálogo Security Settings - Internet Zone é aberta.

5. Rolar para a categoria Script.

   Localize o Script ativo.

   Clique na opção Ativar ou Solicitar.

6. Clique em OK na caixa de diálogo Security Settings - Internet Zone.

   A caixa de diálogo Security Settings - Internet Zone é fechada.

7. Clique em OK na caixa de diálogo Internet Options.

   Esta caixa de diálogo é fechada e a opção Script ativo é aplicada.

Observação: se esta solução não corrigir o problema, consulte o administrador do sistema para verificar se os outros programas, como programas antivírus ou de firewall, não estão bloqueando os scripts ativos, os controles ActiveX ou os programas do Java.

A mensagem Credenciais inválidas é exibida ao adicionar nós

Válido em plataformas Windows.

Sintoma:

A seguinte mensagem é exibida ao tentar adicionar nós para a tela Nós:

```
Credenciais inválidas.
```

Solução:

Este problema ocorre nas seguintes condições:

- As credenciais especificadas na caixa de diálogo Adicionar nós estão incorretas.
- O horário no nó não é o mesmo que o horário no servidor de aplicativos.

Para resolver esse problema, faça o seguinte:

1. Efetue logon no servidor do aplicativo e, em seguida, efetue logon no aplicativo.
2. Na página inicial, selecione Nó na Barra de navegação.

   A tela Nó é exibida.

3. Na barra de ferramentas Nó, clique em Adicionar e, em seguida, clique em Adicionar nó por IP/nome no menu pop-up.

   A caixa de diálogo Adicionar nó por IP/Nome é aberta.

4. Preencha os campos abaixo na caixa de diálogo Adicionar nó por do IP/Nome:
   - **IP/Nome do nó** - permite especificar o endereço IP ou o nome do nó.
   - **Descrição** - permite especificar uma descrição para o nó.
   - **Nome de usuário -** permite especificar o nome de usuário necessário para fazer logon no nó.
   - **Senha -** permite especificar a senha necessária para fazer logon no nó.

   Clique em Validar.
5. Se a mensagem Credenciais inválidas for exibida, faça o seguinte:
   a. Verifique se você especificou as credenciais corretas na caixa de diálogo Adicionar nós e clique em Validar.
   b. Se a mensagem Credenciais inválidas for exibida, verifique se o horário do sistema operacional no servidor de aplicativos é o mesmo que o do sistema operacional no nó.

      Observação: os horários do sistema operacional podem residir em diferentes fusos horários. No entanto, os horários do sistema operacional vezes não podem ser de datas diferentes. Verifique se a data do sistema operacional no nó não corresponde a mais de um dia calendário anterior ou posterior à data do sistema operacional no servidor do aplicativo.

Mensagens de credenciais inválidas no Windows XP

Válido em computadores que executam sistemas operacionais Windows XP.

Sintoma:

Ao adicionar nós com base no Windows XP pela tela Nó, a seguinte mensagem será exibida:

```
Credenciais de usuário inválidas.
```

Solução:

Sob várias condições, o Gerenciador do CA ARCserve Central Protection não pode adicionar nós com base no Windows XP com a opção de pasta Compartilhamento Simples de Arquivo do Windows especificada. Para resolver esse problema, faça o seguinte:

1. Efetue logon no nó do Windows XP e abra o Windows Explorer.
2. No menu Ferramentas, clique em Opções de pasta.

   A caixa de diálogo Opções de pasta é aberta.
3. Clique em Exibir e role até a opção Usar compartilhamento de arquivo simples (recomendável).
4. Limpar a marca de seleção de Usar compartilhamento de arquivo simples (recomendado) e clique em OK.

   O compartilhamento simples de arquivo está desativado.
5. Efetue logon no servidor do Gerenciador do CA ARCserve Central Protection e, em seguida, adicione o nó.

Erros de acesso negado ocorrem ao adicionar um nó por IP/nome

Válido em todos os sistemas operacionais Windows com suporte ao UAC (User Account Control - Controle de Conta de Usuário).

Observação: o Windows Vista, o Windows Server 2008, o Windows Server 2008 R2 e o Windows 7 oferecem suporte ao UAC.

Sintoma:

Ao adicionar nós a partir da caixa de diálogo Adicionar nó por IP/nome usando uma nova conta de usuário do Windows que é integrante do grupo de administradores, a seguinte mensagem é exibida:

```
Acesso negado. Verifique se o usuário tem privilégio de administrador e se o acesso ao Registro remoto não está bloqueado por uma diretiva de segurança local da máquina adicionada.
```

O resultado disso é que você não pode adicionar o nó.

Solução:

Você pode esperar este comportamento quando o UAC está ativado em computadores executando o sistema operacional Windows com suporte ao UAC. O UAC é um recurso do Windows que permite apenas que a conta de administrador efetue logon no computador a partir de um local remoto. A solução para esse comportamento é executar as etapas a seguir:

Siga estas etapas:

1. Efetue logon no nó usando a conta de administrador.
2. Abra o Painel de Controle do Windows.
3. Abra Contas de Usuário.
4. Na tela Fazer alterações na conta de usuário, clique em Alterar configurações de Controle de Conta de Usuário e, em seguida, execute um dos seguintes procedimentos:
   - **Windows Vista e Windows Server 2008:** na tela Fazer alterações na conta de usuário, clique em Ativar ou desativar o Controle de Conta de Usuário. Em seguida, na tela Ativar o Controle de Conta de Usuário (UAC) para tornar o computador mais seguro, desmarque a caixa de seleção ao lado de Utilizar o Controle de Conta de Usuário (UAC) para ajudar a proteger o computador e clique em OK.

     Reinicie seu computador para aplicar as alterações ao UAC.
   - **Windows Server 2008 r2 e Windows 7:** na tela Definir quando deverá ser notificado sobre alterações no computador, mova o controle deslizante de Sempre notificar para Nunca notificar. Clique em OK e feche o Painel de controle do Windows.

     Reinicie seu computador para aplicar as alterações ao UAC.

5. Após a reinicialização do computador, verifique se as seguintes configurações foram aplicadas ao nó do CA ARCserve D2D:
   - O serviço do Windows Server está em execução.
   - O serviço Compartilhamento de arquivo e impressora tem permissão para se comunicar através do firewall do Windows.
   - Quando o nó não é necessário para o ingresso em um domínio, o Serviço de logon de rede tem permissão para se comunicar através do firewall do Windows.
   - O valor de Diretiva de segurança local, Diretivas locais, Opções de segurança e Acesso à rede: modelo de compartilhamento e segurança para contas locais é Clássico.
6. Verifique se a seguinte configuração foi aplicada no servidor do Protection Manager:
   - O valor de Diretiva de segurança local, Diretivas locais, Opções de segurança e Segurança de rede: o nível de autenticação do LAN Manager é Enviar LM e NTLM - use a segurança da sessão NTLMv2, se estiver negociada.

Erro de certificado é exibido ao efetuar logon no aplicativo

Válido em plataformas Windows.

Sintoma:

A seguinte mensagem é exibida na janela do navegador ao efetuar logon no aplicativo:

- Internet Explorer:

  `Há um problema com o certificado de segurança do site.`

- Firefox:

  `Esta conexão não é confiável.`

- Chrome:

  `O certificado de segurança do site não é confiável.`

Se você especificar uma opção que permita continuar com o site, será possível efetuar logon no aplicativo com êxito. No entanto, você encontrará este comportamento toda vez que efetuar logon no aplicativo.

Solução:

Este comportamento ocorre ao especificar o uso de HTTPS como o protocolo de comunicação. Para corrigir esse problema temporariamente, clique no link na janela do navegador que permite continuar com o site. No entanto, da próxima vez que você efetuar logon no aplicativo, você verá esta mensagem novamente.

O protocolo de comunicação HTTPS fornece um nível maior de segurança do que o protocolo de comunicação HTTP. Caso deseje continuar a se comunicar usando o protocolo de comunicação HTTPS, é possível adquirir um certificado de segurança do VeriSign e instalar o certificado no servidor do aplicativo. Como opção, é possível alterar o protocolo de comunicação usado pelo aplicativo para HTTP. Para alterar o protocolo de comunicação para HTTP, faça o seguinte:

1. Faça logon no servidor onde instalou o aplicativo.
2. Vá para o seguinte diretório:

   `C:\Arquivos de programas\CA\ARCserve Central Applications\BIN`
3. Execute o seguinte arquivo em lotes:

   `ChangeToHttp.bat`
4. após executar este arquivo, abra o Gerenciador de servidores do Windows.

   Reinicie o seguinte serviço:

   `Serviço do CA ARCserve Central Applications`

Falha no processo de sincronização do CA ARCserve Backup

Válido em plataformas Windows.

Sintoma:

Ocorre falha no processo de sincronização do CA ARCserve Backup falhar e pode ser exibido no Log de exibição.

Solução:

O processo de sincronização do CA ARCserve Backup pode falhar quando não houver espaço em disco suficiente para armazenar temporariamente os dados da sincronização (arquivos de despejo). Por padrão, o aplicativo armazena os arquivos de despejo no diretório ARCserve_Central_Applications_Home\ASBUSync

Se houver um limite para a quantidade de espaço livre no disco em C:\arquivos de programas, e os arquivos contidos em ASBUSync consumirem mais do que a quantidade de espaço livre no disco, o aplicativo não poderá recuperar os dados de despejo do banco de dados do CA ARCserve Backup necessários para concluir o processo de sincronização. Como resultado, o processo de sincronização do CA ARCserve Backup falha.

Opcionalmente, o aplicativo permite especificar um local diferente para armazenar os dados da sincronização do CA ARCserve Backup. Para corrigir ou evitar este problema, faça o seguinte:

1. Efetue logon no servidor do Gerenciador do CA ARCserve Central Protection.
2. Abra o editor de registro do Windows e procure o seguinte:

   `HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve Central Application\CM`

3. Clique com o botão direito do mouse em CM, selecione Novo e clique em String Value no menu pop-up.

   Nomeie a chave como segue:

   `ARCserveSyncPath`

4. Clique com o botão direito do mouse em ARCserveSyncPath e clique em Modificar no menu pop-up.

   A caixa de diálogo Editar Cadeia de Caracteres é aberta.

5. No campo Value Data, especifique o local alternativo onde deseja armazenar os dados da sincronização do CA ARCserve Backup.

   Clique em OK.

O local alternativo é especificado.

Operações de reimplantação do CA ARCserve D2D falham

Válido em plataformas Windows.

Sintoma:

Ao fazer a reimplantação do CA ARCserve D2D para os nós, o processo de implantação não é concluído com êxito. Esse sintoma se tornará evidente quando um dos seguintes eventos ocorrer:

- Uma das seguintes mensagens for exibida em Status da implantação na caixa de diálogo Implantação do D2D:

  `O usuário não efetuou logon com êxito.`

  `A mesma versão, uma versão mais recente ou uma versão não suportada deste produto está instalada no computador de destino. Antes de instalar a versão atual do produto, é necessário desinstalar a versão anterior.`

  `O programa de instalação não pode copiar os arquivos para o computador remoto.`

- O nó não é exibido na tela Nó.
- O nó é exibido na tela Nó com um status incorreto. Por exemplo, o ícone é exibido na tela Nó, ou o ícone não é exibido na tela Nó.

Solução:

Esses eventos ocorrem nas seguintes condições:

- O serviço web do CA ARCserve Central Applications é interrompido ou reiniciado durante o processo de implantação e o servidor de destino não foi reiniciado após a instalação do CA ARCserve D2D.
- O servidor do CA ARCserve Central Applications é reiniciado durante o processo de implantação e o servidor de destino não foi reiniciado após a instalação do CA ARCserve D2D.

A solução é executar as seguintes ações:

1. Efetue logon no servidor do D2D e reinicie o servidor.
2. Efetue logon no Central Protection Manager e execute uma das seguintes tarefas:
   - Se o nó for exibido na lista de nós na tela Nó e o status não estiver correto, atualize o nó.

     Para atualizar o nó, clique nele e, em seguida, clique em Atualizar no menu pop-up.
   - Se o nó não for exibido na lista de nós na tela Nó, adicione o nó manualmente.

     Para adicionar o nó manualmente, clique em Adicionar na barra de ferramentas e, em seguida, clique em Adicionar nó por IP/nome no menu pop-up.

Resolução de problemas do carregamento da página

Válido em plataformas Windows.

Sintoma:

As seguintes mensagens de erro podem ser exibidas em janelas de navegador ao efetuar logon em nós do CA ARCserve Central Applications, CA ARCserve D2D e servidores de monitoramento.

Mensagem 1:

```
Os erros nesta página podem fazer com que ela funcione incorretamente.
```

Mensagem 2:

```
!
```

Solução:

As páginas da web podem não ser carregadas corretamente por vários motivos. A tabela a seguir descreve os motivos comuns e as respectivas ações corretivas:

Razão	Ação corretiva
Há problemas com o código fonte HTML subjacente.	Atualize a página da web e tente novamente.
Sua rede bloqueia o Script ativo, ActiveX, ou os programas Java.	Permita que seu navegador use Script ativo, ActiveX ou programas Java.
Seu aplicativo antivírus está configurado para examinar arquivos temporários da Internet e programas cujo download foi concluído.	Filtre o aplicativo antivírus para permitir arquivos relacionados à Internet associados a páginas da web do CA ARCserve Central Applications.
O mecanismo de script instalado em seu computador está corrompido ou desatualizado.	Atualize o mecanismo de script.
A placa de vídeo instaladas no computador estão corrompidas ou desatualizadas.	Atualize-as.
O componente DirectX instalado em seu computador está corrompido ou desatualizado.	Atualize-o.

Caracteres sem sentido são exibidos no navegador do Windows ao acessar o CA ARCserve Central Applications

Válido em todos os sistemas operacionais Windows. Todos os navegadores afetados.

Sintoma:

Ao efetua logon no CA ARCserve Central Applications, caracteres sem sentido aparecem na área de conteúdo da janela do navegador.

Solução:

Este problema ocorre ao instalar o CA ARCserve Central Applications usando a comunicação HTTPS e ao tentar acessar o CA ARCserve Central Applications usando a comunicação HTTP. O componente subjacente dos serviços web do CA ARCserve Central Applications não oferece suporte ao recurso para converter URLs HTTP para URLs HTTPS. Como resultado, os caracteres sem sentido aparecem na janela do navegador. Por exemplo:

Para corrigir esse problema, acesse o CA ARCserve Central Applications usando o HTTPS ao instalar ou configurar aplicativos para se comunicar usando o HTTPS.

Os nós não aparecem na tela Nó após alterar o nome do nó

Válido em plataformas Windows.

Sintoma:

O nome do host do nó foi alterado depois que ele foi adicionado à tela Nó. O nó não será mais exibido na tela Nó.

Solução:

Esse comportamento é esperado. O Gerenciador do CA ARCserve Central Protection mantém o nome do nó que foi adicionado da tela Nó. Ao renomear o nó, o aplicativo não poderá detectá-lo. Do mesmo modo, o nó não será exibido na tela Nó.

Para exibir os nós renomeados na tela, proceda da seguinte maneira:

1. Renomeie o nó.
2. Abra a tela Nó e exclua o nó (na página 63) que foi renomeado.
3. Adicione o nó (na página 57) usando seu novo nome.

O Gerenciador do CA ARCserve Central Protection não consegue se comunicar com o serviço web do CA ARCserve D2D em nós remotos

Válido em sistemas operacionais Windows.

Sintoma:

O Gerenciador do CA ARCserve Central Protection não consegue se comunicar com o serviço web do CA ARCserve D2D em nós remotos.

Solução:

A tabela a seguir descreve os motivos pelos quais o Gerenciador do CA ARCserve Central Protection não consegue se comunicar com o serviço web do CA ARCserve D2D em nós remotos e a ação corretiva correspondente:

Causa	Ação corretiva
A rede não está disponível ou não está estável ao aplicar diretivas.	Verifique se a rede está disponível e estável e tente novamente.
O computador do CA ARCserve D2D não pôde lidar com a carga quando o aplicativo tentou comunicar-se com o nó.	Verifique se a CPU no nó remoto do CA ARCserve D2D está em um estado normal e tente novamente.
O serviço do CA ARCserve D2D no nó remoto não estava em execução ao aplicar as diretivas.	Verifique se o nó remoto do CA ARCserve D2D está em execução e tente novamente.
O serviço do CA ARCserve D2D não está se comunicando adequadamente.	Reinicie este serviço do CA ARCserve D2D no nó remoto e tente novamente.

Os nós não são gerenciados após a implantação do D2D

Válido em plataformas Windows.

Sintoma:

Ao implantar o CA ARCserve D2D em um nó de um servidor local ou remoto, o nó é adicionado ao grupo de nós, mas o status NÃO é gerenciado.

Esse problema ocorre na presença de uma das seguintes condições:

- O CA ARCserve D2D foi implantado em um nó remoto sem reinicialização.
- O CA ARCserve D2D foi implantado no servidor local do CA ARCserve Central Applications com ou sem reinicialização.

Solução:

Para corrigir esse problema, reinicie o servidor do CA ARCserve D2D e atualize as informações do nó do CA ARCserve D2D no Gerenciador do CA ARCserve Central Protection. O status torna-se gerenciado.

Como definir programações para a exclusão de dados do nó

Válido em plataformas Windows.

Sintoma:

Por padrão, a programação de exclusão de dados do nó é configurada para limpar dados de nós excluídos todos os dias às 2:00. Eu gostaria de personalizar a programação para a exclusão de vários dados.

Solução:

Para criar uma programação personalizada para a exclusão de dados de nós, defina o valor da chave do Registro CA ARCserve Central Applications\CM\ShowDeleteNodeConfigurationUI to 1. Definir a chave do Registro como 1 adiciona a guia Configuração de exclusão de dados do nó no painel Configuração no aplicativo do Gerenciador do CA ARCserve Central Protection para alterar a programação.

Observação: para acessar o Registro, efetue logon diretamente no servidor do Gerenciador do CA ARCserve Central Protection e vá para Iniciar > Executar > Regedit.

Os serviços do banco de dados do CA ARCserve Central Applications não iniciam

Válido em plataformas Windows e bancos de dados do Microsoft SQL Server e Microsoft SQL Server Express Edition.

Sintoma:

Ao iniciar ou reiniciar o servidor do Gerenciador do CA ARCserve Central Protection onde o banco de dados do CA ARCserve Central Applications está instalado, os serviços do banco de dados do CA ARCserve Central Applications não iniciam.

Solução:

Ao iniciar um computador, os serviços relatam o status de inicialização para o sistema operacional. Quando os serviços não relatam um status para o sistema operacional em um período de tempo predeterminado (ou o período de tempo limite), o Windows interrompe os serviços. Por padrão, quando os serviços do CA ARCserve Central Applications não relatam um status para o Windows em até 30 segundos do horário de início, o Windows interrompe o serviço do banco de dados do CA ARCserve Central Applications. Você provavelmente irá se deparar com esse tipo de problema quando o banco de dados for instalado em um servidor que não tem recursos suficientes. No entanto, é possível evitar esse problema ao aumentar o período de tempo limite para inicialização. Para aumentar o período de tempo limite, proceda da seguinte maneira:

1. Abra o editor de registro do Windows e procure a seguinte chave:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control`
2. Clique com o botão direito do mouse em Controle, aponte para Novo e clique em Chave no menu pop-up.

   Uma chave denominada Nova Chave #1 é criada.
3. Renomeie a Nova chave #1 para ServicesPipeTimeout.
4. Clique com o botão direito do mouse em ServicesPipeTimeout e clique em Modificar no menu pop-up.

   A caixa de diálogo Editar Valor DWORD é aberta.
5. No campo de dados Valor, especifique o valor que deseja definir para o período de tempo limite. Expresse o valor em milissegundos. Por exemplo, para definir o período de tempo limite para 60 segundos, especifique 60000 no campo de dados Valor.

   Observação: um segundo é igual a 1000 milissegundos.

   Clique em OK.

   O período de tempo limite é aplicado.
6. Para aplicar as alterações ao Windows, reinicie o computador.

Ocorrem diversos erros de conexão ao salvar ou atribuir uma diretiva ao servidor do CA ARCserve D2D

Válido em todas as plataformas Windows.

Sintoma:

Ao tentar salvar ou atribuir uma diretiva a um servidor do CA ARCserve D2D, a mensagem de erro a seguir é exibida:

```
Falha ao validar o destino do backup. Não são permitidas várias conexões com um servidor ou recurso compartilhado pelo mesmo usuário, usando mais de um nome de usuário. Desconecte todas as conexões anteriores com o servidor ou recurso compartilhado e tente novamente.
```

Solução:

Se a mensagem anterior for exibida ao tentar salvar ou atribuir uma diretiva a um servidor do CA ARCserve D2D, as seguintes ações corretivas pode ajudá-lo a resolver o problema:

- Marque o campo Nome de usuário com o nome do usuário\nome do computador (ou domínio).
- Vá para o servidor remoto onde a pasta compartilhada está hospedada e exclua todas as sessões do servidor do CA ARCserve Central Applications ou do servidor do CA ARCserve D2D. Siga um destes procedimentos para excluir as sessões:
  - Execute a linha de comando a seguir:

    ```
    net session \\machinename /delete
    ```

  - Vá para o seguinte diretório para desconectar a sessão:

    ```
    Compmgmt.msc > Ferramentas do sistema > Pastas compartilhadas > Sessões > Desconectar sessão
    ```

- Verifique se você está usando o mesmo nome de usuário para acessar a pasta compartilhada remota.
- Salve e implante a diretiva novamente.

Sincronização de dados e operações de implantação de diretiva falham

Válido em plataformas Windows.

Sintoma:

A seguinte mensagem é exibida no log de atividades após o início da operação de sincronização de dados do CA ARCserve D2D:

```
O aplicativo não pode efetuar logon no serviço do CA ARCserve D2D.
```

A caixa de mensagem a seguir é exibida quando você implanta uma diretiva no nó:

```
Falha ao implantar diretiva (falha ao estabelecer conexão com o nó).
```

Solução:

Esse comportamento ocorre quando você desinstala o CA ARCserve D2D no nó depois que ele foi registrado para o servidor do Gerenciador do CA ARCserve Central Protection e, em seguida, reinstala o CA ARCserve D2D manualmente no nó. Esse comportamento não ocorre ao usar o utilitário de implantação do Gerenciador do CA ARCserve Central Protection para reinstalar o CA ARCserve D2D no nó.

A solução para esse comportamento é atualizar o nó na tela Nó. Para atualizar o nó, clique nele e, em seguida, clique em Atualizar no menu pop-up. Em seguida, preencha os campos necessários na caixa de diálogo Atualizar nó.

Número do erro na Solução de problemas

A tabela a seguir descreve os números de erros exibidos como mensagens pop-up ao adicionar ou atualizar nós usando o Gerenciador do CA ARCserve Central Protection.

Número do erro	Descrição	Solução possível
12884901933	Não é possível estabelecer conexão com o serviço do CA ARCserve D2D em *** e número do erro é 12884901933. Verifique se todas as entradas para o nó estão corretas e se o serviço do CA ARCserve D2D está em execução.	Verifique o seguinte: ■ O serviço do CA ARCserve D2D está em execução no nó. ■ O nome do host, o endereço IP e o protocolo de comunicação especificados para o nó estão correto. ■ O serviço web do CA ARCserve D2D no nó está em execução, e não aparece bloqueado devido ao fato do DNS conseguir resolver o endereço IP do nó. ■ O serviço web do CA ARCserve D2D no nó está em execução, e o firewall do Windows, ou qualquer outro firewall não está bloqueando a comunicação. ■ O cabo de rede está conectado e o nó está funcionando corretamente. ■ O usuário conectado ao nó tem as permissões necessárias para se comunicar usando uma rede sem fio.
12884901935	Não é possível estabelecer conexão com o serviço do CA ARCserve Backup em *** e número do erro é 12884901935. Verifique se todas as entradas para o nó estão corretas e se o serviço do CA ARCserve Backup está em execução.	Verifique se o serviço do CA ARCserve Communication Foundation está em execução no nó.
12884901936	Não é possível estabelecer conexão com o serviço do CA ARCserve Backup em *** e número do erro é 12884901936. Verifique se o CA ARCserve Central Applications oferece suporte para a versão do serviço do CA ARCserve Backup instalado no nó.	Verifique o seguinte: ■ O CA ARCserve Central Applications oferece suporte para a versão do serviço do CA ARCserve Backup instalado no nó. ■ O serviço do CA ARCserve Communication está em execução no nó

O link Adicionar nova guia não é iniciado corretamente no Internet Explorer 8 e 9 nem no Chrome

Válido no Windows

Sintoma:

Ao adicionar o link de uma nova guia à barra de navegação especificando o URL de um HTTPS, as seguintes mensagens de erros serão exibidas quando eu clicar na nova guia:

- Internet Explorer 8 e 9:

  `O conteúdo foi bloqueado porque não foi assinado por um certificado de segurança válido.`

- Chrome:

  `Esta página web não está disponível.`

Solução:

Para corrigir esse problema no Internet Explorer, faça o seguinte:

- Internet Explorer 8:

  Clique na barra de mensagens e selecione "Exibir Conteúdo Bloqueado".

- Internet Explorer 9:

  Clique no botão "Mostrar conteúdo" na barra de mensagens na parte inferior da página. A página é atualizada e o link para a guia adicionada é aberto com êxito.

Para corrigir esse problema no Chrome, execute as seguintes etapas:

Etapa 1 - Exportar certificado:

1. Abra uma nova guia no Chrome e digite o URL do HTTPS.

   A mensagem de aviso "The site's security certificate is not trusted!" é exibida.

2. Na barra de endereços, clique no cadeado com 'X'.

   Uma janela pop-up é exibida com o link Certification Information.

3. Clique nesse link.

   A caixa de diálogo Certificate é aberta.

4. Clique na guia Details e, em seguida, clique em Copy to File, para salvar o certificado em seu computador local.

   A caixa de diálogo do Assistente para exportação de certificados é exibida.

5. Clique em Next para selecionar o formato deseja usar para exportar o arquivo.

   Observação: o binário X.509 codificado por DER (*.CER) vem selecionado por padrão.

6. Clique em Next para ir para o local em que deseja salvar o certificado.
7. Clique em Next para concluir o Certificate Export Wizard e, em seguida, clique em Finish.

O certificado é exportado com êxito.

Etapa 2 - Importar certificado:

1. Abra a caixa de diálogo Tools Options no Chrome.

   A tela Options é aberta.

2. Selecione a opção Under the Hood e clique em Manage Certificates from HTTPS/SSL.

   A caixa de diálogo Certificates é aberta.

3. Clique em Importar.

   A caixa de diálogo do Assistente para importação de certificados é exibida.

4. Clique em Next para ir para o certificado salvo no seu computador local.
5. Clique em Avançar para abrir o Armazenamento de certificados.

   A caixa de diálogo Certificate Store é aberta.

6. Clique em Browse para abrir a caixa de diálogo Select Certificate Store.

   A caixa de diálogo Select Certificate Store é aberta.

7. Selecione as Trusted Root Certification Authorities na lista de arquivos e clique em OK.

   A caixa de diálogo Armazenamento de certificados é aberta.

8. Clique em Next para concluir o Certificate Import Wizard e, em seguida, clique em Finish.

   A caixa de diálogo Security Warning é exibida, indicando que você está prestes a instalar um certificado.

   Clique em Sim para concordar com os termos.

O certificado é importado com êxito.

O link Adicionar nova guia, os feeds de RSS e os comentários de rede social não são iniciados corretamente no Internet Explorer 8 e 9

Válido no Windows

Sintoma:

Para o URL de um HTTPS do CA ARCserve Central Applications:

Ao adicionar o link de uma nova guia à barra de navegação especificando o URL de um HTTP, as seguintes mensagens de erro serão exibidas quando eu clicar na nova guia e no link Comentários:

```
A navegação para a página da web foi cancelada.
```

Além disso, os feeds de RSS não são exibidos.

Observação: o link Comentários também exibe a mensagem de erro, mesmo que você não selecione o link da nova guia.

Solução:

Para resolver esse problema, faça o seguinte:

- Internet Explorer 8:

  Após efetuar logon, clique em Não na mensagem pop-up de aviso de segurança, "Deseja exibir apenas o conteúdo oferecido de forma segura por esta página da Web?". Clicar em Não permite a entrega de conteúdo que não seja seguro em sua página da web.

- Internet Explorer 9:

  Clique no botão "Mostrar todo o conteúdo" na barra de mensagens na parte inferior da página. A página é atualizada e o link da guia adicionada é aberto com êxito.

Os caracteres em servidores localizados aparecem ilegíveis no Console de alarmes do Nimsoft UMP

Válido no Windows.

Sintoma:

Os caracteres das mensagens de alerta recebidas de servidores localizados são exibidos como texto ilegível no Console de alarmes do UMP (Nimsoft Unified Monitoring Portal).

Solução:

Este comportamento ocorre quando o conjunto de caracteres em execução no servidor que enviar alertas é diferente do conjunto de caracteres em execução no servidor do Nimsoft. A solução para esse comportamento é configurar o servidor para usar a codificação UTF-8. Para configurar o servidor para usar a codificação UTF-8, faça o seguinte:

1. Verifique se o mecanismo está configurado para usar -Dfile.encoding=utf-8 como um parâmetro de inicialização.
2. Verifique se a opção extra de argumentos wasp do Java VM está definida como –Dfile.encoding=utf-8.

Observação: para obter mais informações, consulte a documentação do Nimsoft.

Índice remissivo

D

E

F

G

I

L

M